IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. HAOYANG YU, *et al*.	No. 19-cr-10195-WGY

APPENDIX B
PRESS ARTICLES AND RELEASES CITED IN MEMORANDUM IN SUPPPORT OF MOTION TO DISMISS INDICTMENT DUE TO UNCONTITUTIONAL SELECTIVE ENFORCEMENT AND PROSECUTION

* * * * *

The Washington Post
Democracy Dies in Darkness

Scrutiny of Chinese American scientists raises fears of ethnic profiling

By **Nick Anderson**

July 19, 2019 at 8:13 p.m. EDT

Two years ago, the director of the National Institutes of Health hailed genetic research from Emory University as a promising advance in the quest to treat Huntington's disease, a devastating neurological disorder.

A Chinese-born couple, Xiao-Jiang Li and Shihua Li, both Emory professors, were among the authors of the study on gene editing in mice. NIH Director Francis S. Collins called the results "reassuring news" as scientists explore the "potential curative power" of gene editing. Published in the Journal of Clinical Investigation, the study was a prime display of the globalization of science and the deep Chinese connections to U.S. higher education.

Now, the Lis are booted from Emory, their laboratory shuttered, their tale an example of the rising scrutiny of ethnic Chinese scientists that has rattled campuses from coast to coast.

Support journalism you can trust when it matters most.
Get one year for $29

The university fired them abruptly in May — 23 years after they arrived at the prestigious Emory School of Medicine in Atlanta. It charged that the professors failed to fully disclose foreign sources of research funding and the extent of their work for institutions and universities in China. Both scientists are naturalized U.S. citizens.

Xiao-Jiang Li, who held tenure at Emory as a distinguished professor of human genetics, disputes the university's account. "I routinely disclosed my Chinese affiliations and Chinese funding in my publications," he said recently in an email from China.

The couple's departure underscores the roiling debate over how to preserve the culture of free academic exchange and international cooperation that is a hallmark of American universities, while preventing China and other nations from abusing that trust.

AD

In the research arena, federal officials in recent years have sounded alarms about violations of funding disclosure rules, breaches of confidential grant proposals and even outright espionage orchestrated by the Chinese government. NIH has sent letters about potential violations to more than 60 research institutions within the past year, according to Michael S. Lauer, NIH deputy director for extramural research, questioning the conduct of "well over 100" scientists.

The FBI and other federal agencies are working with universities to tighten enforcement of rules and laws.

Critics denounce the crackdown as ethnic profiling that will weaken science and stigmatize innocent researchers. Advocates call it a prudent response to an emerging threat.

AD

In April, FBI Director Christopher A. Wray said China is taking "a societal approach

to stealing innovation in any way it can" from universities and other sources. "I do think that the academic sector needs to be much more sophisticated and thoughtful about how others may exploit the very open, collaborative research environment that we have in this country," Wray told the Council on Foreign Relations in Washington.

Warnings about malign foreign influence on college campuses come as President Trump has sparred with China over tariffs and trade and his administration has moved to limit visas for Chinese graduate students in certain research fields. Lawmakers on Capitol Hill have proposed bills to prevent academic espionage.

It is hard to overstate the importance of China for U.S. colleges and universities. China is by far the leading supplier of international students to the United States, with more than 130,000 graduate students and 148,000 undergraduates enrolled in 2017-2018. Those students bring vital tuition dollars into the U.S. system. China's own universities are also rapidly developing research capacity that the United States cannot ignore. New York and Duke universities have opened outposts in China.

AD

Now, some academics in the United States worry about a repeat of the "Red Scare" over communist infiltration that Sen. Joseph R. McCarthy (R-Wis.) fomented in the

1950s.

Yiguang Ju, a professor of mechanical and aerospace engineering at Princeton University, said he senses "increasing fear of a new McCarthyism" if conflicts with China intensify. Ju, 55, earned a bachelor's degree in his native China and a doctorate in Japan before moving to the United States in 2001 and eventually becoming a naturalized U.S. citizen.

He spoke in late June at the China Institute, a cultural and educational organization in New York. The event was called "The New Normal: The perils of being a Chinese scientist in the U.S."

AD

Ju said faculty have long abided by rules protecting intellectual property and controlling the export of sensitive technology. Now, many are frustrated, he said, at questions about foreign influence in academia. They want clear guidance. "This is the tough part: Where do you draw the line between foreign influence and academic exchange?" he asked.

Ju, who receives federal funding for his research on combustion, energy and propulsion, said in a telephone interview that he routinely collaborates with peers from Germany, France, Ireland, Britain and elsewhere. Sometimes, Chinese scholars visit his lab. "People look at things from different angles," he said. "It helps you think outside the box."

NIH officials say the rules they are enforcing have long been clear: Scientists who seek federal funding must disclose professional affiliations and sources of financial support, and they must protect the confidentiality of grant proposals submitted for peer review. Those proposals provide a precious window into cutting-edge science.

AD

"To have faith in the system, the system has to run according to agreed-upon rules and norms of behavior," said Lauer, who oversees more than $25 billion a year in NIH grants. "This is not new."

The rules are meant to uphold transparency, prevent the loss of intellectual property and ensure conflicts of interest do not taint research findings.

The FBI alerted NIH to potential rule violations in 2016, Lauer said. Many cases arose through information from the FBI or internal NIH reviews, he said, and others are based on tips from whistleblowers. Universities have also notified NIH of problems they have discovered on their own.

Not all of those identified as potential rule-breakers were of Chinese descent, Lauer said, but the majority were. "It's not based on ethnicity," he said. "It's based on specific behavior."

AD

The investigations have led to the ouster of the Lis and three scientists of Asian descent from the University of Texas MD Anderson Cancer Center, according to news reports. Lauer confirmed a June 26 report from the journal Science that universities have quietly fired others and refunded the government hundreds of thousands of dollars in grants. He declined to elaborate.

The Lis, who declined to provide their ages, have been in the United States for decades and were part of a wave of Chinese immigrants who joined American faculties in the past 30 years. Xiao-Jiang Li and Shihua Li both earned medical degrees from Jiangxi Medical College in China in 1982, according to their résumés. Xiao-Jiang Li earned a doctorate in pharmacology in 1991 from a school then named Oregon Health Sciences University. He was on the faculty of Johns Hopkins University before joining Emory as an assistant professor in 1996. Shihua Li started at Emory that year as a senior research associate.

After settling in Georgia, the couple maintained ties to China. Xiao-Jiang Li notes on a résumé prepared for NIH that he was honored in 2010 as a professor in the "Thousand Talents" program, an initiative to attract top scientists to work in China. He also kept professional ties to Chinese institutions, including a recent appointment at Jinan University in Guangzhou.

AD

Thousand Talents has drawn fire in recent years. Critics call the program a ploy to help China achieve technological and scientific supremacy. NIH said the program is a "known prominent player."

Emory declined to make officials available to discuss why the Lis were terminated. Shihua Li declined to comment. Her husband said in an email that he has disclosed to Emory his time and the nature of his work in China every year since 2012. He said the couple's NIH-funded projects had no overlap with his research in China.

"We were not charged with any crimes or accused of stealing technology, and were not contacted by FBI either," Xiao-Jiang Li said.

An attorney for Xiao-Jiang Li, Peter R. Zeidenberg, said Li was fired before being given a chance to respond to evidence against him. "He was a tenured professor," Zeidenberg said. "No due process."

Emory replied in an email: "Dr. Li was provided an opportunity to respond. Under Emory policies, he has the opportunity to appeal the decision and he has done so."

For Emory and other universities, the stakes in these investigations are high. They seek to ensure they will not lose access to government funding, but they do not want to alienate campus communities that value what foreigners and immigrants contribute.

"It is important to note that Emory remains committed to the free exchange of ideas and research and to our vital collaborations with researchers from around the world," Emory said.

Denis Wirtz, vice provost for research at Johns Hopkins, lamented what he called a "palpable" level of anxiety among foreign-born scholars. Wirtz — himself a Belgian immigrant — said universities must reassure them that they are welcome, or else

they will leave. "These people have options," he said. Pushing them out would be "really shooting ourselves in the foot."

The president of the Massachusetts Institute of Technology, L. Rafael Reif, said universities "must take great care not to create a toxic atmosphere of unfounded suspicion and fear."

"Looking at cases across the nation, small numbers of researchers of Chinese background may indeed have acted in bad faith, but they are the exception and very far from the rule," Reif said in a June 25 email to the university. "Yet faculty members, post-docs, research staff and students tell me that, in their dealings with government agencies, they now feel unfairly scrutinized, stigmatized and on edge — because of their Chinese ethnicity alone."

Xiaoxing Xi, 61, a Temple University physicist who is Chinese American, says he knows well what it is like to be stigmatized. In 2015, FBI agents stormed his house and arrested him in front of his wife and daughters on an accusation that he had illicitly shared information about a superconductor device with colleagues in China. The government, which obtained evidence through intercepted emails, dropped the charges after Xi showed that what he had shared was public knowledge.

Xi is suing the government for damages for what he says was a violation of his constitutional rights that harmed his career. He is also speaking out about the dangers of a security crackdown.

"What happened to me can happen to anybody," he said. "People need to be more aware of this."

The New York Times https://nyti.ms/1MhmTct

U.S. Drops Charges That Professor Shared Technology With China

By Matt Apuzzo

Sept. 11, 2015

WASHINGTON — When the Justice Department arrested the chairman of Temple University's physics department this spring and accused him of sharing sensitive American-made technology with China, prosecutors had what seemed like a damning piece of evidence: schematics of sophisticated laboratory equipment sent by the professor, Xi Xiaoxing, to scientists in China.

The schematics, prosecutors said, revealed the design of a device known as a pocket heater. The equipment is used in superconductor research, and Dr. Xi had signed an agreement promising to keep its design a secret.

But months later, long after federal agents had led Dr. Xi away in handcuffs, independent experts discovered something wrong with the evidence at the heart of the Justice Department's case: The blueprints were not for a pocket heater.

Faced with sworn statements from leading scientists, including an inventor of the pocket heater, the Justice Department on Friday afternoon dropped all charges against Dr. Xi, an American citizen.

It was an embarrassing acknowledgment that prosecutors and F.B.I. agents did not understand — and did not do enough to learn — the science at the heart of the case before bringing charges that jeopardized Dr. Xi's career and left the impression that he was spying for China.

"I don't expect them to understand everything I do," Dr. Xi, 57, said in a telephone interview. "But the fact that they don't consult with experts and then charge me? Put my family through all this? Damage my reputation? They shouldn't do this. This is not a joke. This is not a game."

The United States faces an onslaught from outside hackers and inside employees trying to steal government and corporate secrets. President Obama's strategy to combat it involves aggressive espionage investigations and prosecutions, as well as increased cyberdefenses.

But Dr. Xi's case, coming on the heels of a similar case that was dismissed a few months ago in Ohio, raises questions about whether the Justice Department, in its rush to find Chinese spies, is ensnaring innocent American citizens of Chinese ancestry.

A spokeswoman for Zane D. Memeger, the United States attorney in Philadelphia who brought the charges, did not elaborate on the decision to drop the case. In court documents, the Justice Department said that "additional information came to the attention of the government."

The filing gives the government the right to file the charges again if it chooses. A spokesman for John P. Carlin, the assistant attorney general who is overseeing the crackdown on economic espionage, had no comment on whether Justice Department officials in Washington reviewed the case.

The science involved in Dr. Xi's case is, by any measure, complicated. It involves the process of coating one substance with a very thin film of another. Dr. Xi's lawyer, Peter Zeidenberg, said that despite the complexity, it appeared that the government never consulted with experts before taking the case to a grand jury. As a result, prosecutors misconstrued the evidence, he said.

Mr. Zeidenberg, a lawyer for the firm Arent Fox, represented both Dr. Xi and Sherry Chen, a government hydrologist who was charged and later cleared in the Ohio case. A longtime federal prosecutor, Mr. Zeidenberg said he understood that agents felt intense pressure to crack down on Chinese espionage, but the authorities in these cases appeared to have been too quick to assume that their suspicions were justified.

In Dr. Xi's case, Mr. Zeidenberg said, the authorities saw emails to scientists in China and assumed the worst. But he said the emails represented the kind of international academic collaboration that governments and universities encourage. The technology discussed was not sensitive or restricted, he said.

"If he was Canadian-American or French-American, or he was from the U.K., would this have ever even got on the government's radar? I don't think so," Mr. Zeidenberg said.

The Justice Department sees a pernicious threat of economic espionage from China, and experts say the government in Beijing has an official policy encouraging the theft of trade secrets. Prosecutors have charged Chinese workers in the United States with stealing Boeing aircraft information, specialty seeds and even the pigment used to whiten Oreo cookie cream.

Other researchers and academics are being closely watched. The F.B.I. is investigating a Chinese-American mapping expert who abruptly resigned from Ohio State University last year and disappeared while working with NASA, The Columbus Dispatch reported this week. In May, the Justice Department charged a Chinese professor and others with stealing acoustics equipment from American companies.

About a dozen F.B.I. agents, some with guns drawn, stormed Dr. Xi's home in the Philadelphia suburbs in May, searching his house just after dawn, he said. His two daughters and his wife watched the agents take him away in handcuffs on fraud charges.

"Unfortunately I think this is influenced by the politics of the time," he said. "But I think it's wrong. We Chinese-Americans, we contribute to the country, to the national security, to everything."

Temple University put him on administrative leave and took away his title as chairman of the physics department. He was given strict rules about who at the school he could talk to. He said that made it impossible for him to continue working on a long-running research project that was nearing completion.

Dr. Xi, who came to the United States in 1989 and is a naturalized citizen, was adamant that he was innocent. But it was only when he and his lawyers reviewed the government's evidence that they understood what had happened. "When I read it, I knew that they were mixing things up," Dr. Xi said.

His lawyers contacted independent scientists and showed them the diagram that the Justice Department said was the pocket heater. The scientists agreed it was not.

In a sworn affidavit, one engineer, Ward S. Ruby, said he was uniquely qualified to identify a pocket heater. "I am very familiar with this device, as I was one of the co-inventors," he said.

Last month, Mr. Zeidenberg delivered a presentation for prosecutors and explained the science. He gave them sworn statements from the experts and implored the Justice Department to consult with a physicist before taking the case any further. Late Friday afternoon, the Justice Department dropped the case "in the interests of justice."

"We wish they had come to us with any concerns they had about Professor Xi prior to indicting him, but at least they did listen," Mr. Zeidenberg said.

Dr. Xi choked back tears as he described an ordeal that was agonizing for his family. "I barely came out of this nightmare," he said.

The New York Times https://nyti.ms/2XPRk18

NEWS ANALYSIS

Trump Fans the Flames of a Racial Fire

By Peter Baker

July 14, 2019

WASHINGTON — President Trump woke up on Sunday morning, gazed out at the nation he leads, saw the dry kindling of race relations and decided to throw a match on it. It was not the first time, nor is it likely to be the last. He has a pretty large carton of matches and a ready supply of kerosene.

His Twitter harangue goading Democratic congresswomen of color to "go back" to the country they came from, even though most of them were actually born in the United States, shocked many. But it should have surprised few who have watched the way he has governed a multicultural, multiracial country the last two and a half years.

When it comes to race, Mr. Trump plays with fire like no other president in a century. While others who occupied the White House at times skirted close to or even over the line, finding ways to appeal to the resentments of white Americans with subtle and not-so-subtle appeals, none of them in modern times fanned the flames as overtly, relentlessly and even eagerly as Mr. Trump.

His attack on the Democratic congresswomen came on the same day his administration was threatening mass roundups of immigrants living in the country illegally. And it came just days after he hosted some of the most incendiary right-wing voices on the internet at the White House and vowed to find another way to count citizens separately from noncitizens despite a Supreme Court ruling that blocked him from adding a question to the once-a-decade census.

[*Mr. Trump lashed out again Monday, accusing the women of themselves using "racist hatred."*]

His assumption that the House Democrats must have been born in another country — or that they did not belong here if they were — fits an us-against-them political strategy that has been at the heart of Mr. Trump's presidency from the start. Heading into next year's election, he appears to be drawing a deep line between the white, native-born America of his memory and the ethnically diverse, increasingly foreign-born country he is presiding over, challenging voters in 2020 to declare which side of that line they are on.

"In many ways, this is the most insidious kind of racial demagoguery," said Douglas A. Blackmon, the author of "Slavery by Another Name," a Pulitzer Prize-winning history of racial servitude in America between the Civil War and World War II. "The president has moved beyond invoking the obvious racial slanders of 50 years ago — clichés like black neighborhoods 'on fire' — and is now invoking the white supremacist mentality of the early 1900s, when anyone who looked 'not white' could be labeled as unwelcome in America."

Mr. Trump ritually denies any racial animus or motivations. His fight against illegal immigration, he says, is only about securing the border and protecting the country. He regularly boasts that unemployment among Hispanics and African-Americans has hit record lows. Last week he thanked Robert L. Johnson, the founder of Black Entertainment Television, for crediting his stewardship of the economy.

"I am the least racist person you have ever met," he has said more than once.

But he does not go out of his way to avoid looking like he is, and his string of Twitter posts on Sunday left his own advisers unable or unwilling to defend him. None of six spokespeople for the White House or his campaign initially responded to requests for comment.

One of the only administration officials who was already booked for the Sunday talk shows, Mark Morgan, the acting commissioner of Customs and Border Protection, made clear he wanted no part of it. "You're going to have to ask the president what he means by those specific tweets," he said on "Face the Nation" on CBS.

Republican lawmakers, by and large, did not rush to the president's side on Sunday either, but neither did they jump forward to denounce him. Deeply uncomfortable as many Republicans are with Mr. Trump's racially infused politics, they worry about offending the base voters who cheer on the president as a truth-teller taking on the tyranny of political correctness.

Only in the evening did Mr. Trump respond to the furor, saying that Democrats were standing up for colleagues who "speak so badly of our Country" and "whenever confronted" call adversaries "RACIST."

At that point, Tim Murtaugh, a campaign spokesman for Mr. Trump, responded to a request for comment, saying, "The president pointed out that many Democrats say terrible things about this country, which in reality is the greatest nation on Earth." He did not explain why Mr. Trump told American-born lawmakers to "go back" to countries they were not from.

Other presidents have played racial politics or indulged in stereotypes. Secret tapes of Lyndon B. Johnson and Richard M. Nixon show them routinely making virulently racist statements behind closed doors. Mr. Nixon's Southern strategy was said to be aimed at disenchanted whites. Ronald Reagan was accused of coded racial appeals for talking so much about "welfare queens." George Bush and

his supporters highlighted the case of a furloughed African-American murderer named Willie Horton. Bill Clinton was accused of a racial play for criticizing a black hip-hop star.

But there were limits, even a generation ago, and most modern presidents preached racial unity over division. Mr. Johnson, of course, pushed through the most sweeping civil rights legislation in American history. Mr. Bush signed a civil-rights bill and denounced David Duke, the Ku Klux Klan leader, when he ran for governor of Louisiana as a Republican. His son, George W. Bush, made a point of visiting a mosque just days after the attacks of Sept. 11, 2001, to emphasize that America was not at war with Muslims. Barack Obama invited an African-American Harvard professor and the white police officer who mistakenly arrested him for a "beer summit."

Mr. Trump's history on race has been well documented, from his days as a developer settling a Justice Department lawsuit over discrimination in renting apartments to his public agitation during the Central Park Five case in New York. Jack O'Donnell, the former president of Trump Plaza Hotel and Casino in Atlantic City, later wrote that Mr. Trump openly disparaged others based on race, complaining, for example, that he did not want black men managing his money.

"Trump has not only always been a racist, but anyone around him who denies it, is lying," Mr. O'Donnell said on Sunday. "Donald Trump makes racist comments all the time. Once you know him, he speaks his mind about race very openly."

Mr. Trump, he said, regularly trafficked in racial stereotypes — Jews were good with money, blacks were lazy, Puerto Ricans dressed badly. "White people are Americans to Trump; everyone else is from somewhere else," Mr. O'Donnell said. "He simply denies the reality of how we all immigrated to the United States."

Mr. Trump propelled his way to the White House in part by promoting the false "birther" conspiracy theory that Mr. Obama was actually born in Africa, not Hawaii. He opened his presidential bid in 2015 with an attack on Mexican "rapists" coming across the border (although "some, I assume, are good people") and later called for a ban on all Muslims entering the United States. He said an American-born judge of Mexican heritage could not be fair to him because of his ethnic background.

As president, he complained during meetings that became public that Haitian immigrants "all have AIDS" and said African visitors would never "go back to their huts." He disparaged Haiti and some African nations with a vulgarity and said instead of immigrants from there, the United States should accept more from Norway. He said there were "very fine people on both sides" of a rally to save a Confederate monument that turned deadly in Charlottesville, Va., although he also condemned the neo-Nazis there.

He is only saying what others believe but are too afraid to say, he insists. And each time the flames roar and Mr. Trump tosses a little more accelerant on top. The fire may be hot, but that's the way he likes it.

Center for Strategic and International Studies

TRANSCRIPT

CSIS Event

"China Initiative Conference"

Keynote Address

RECORDING DATE

Thursday, February 6, 2020

TIME

10:00 a.m. EDT

LOCATION

2nd Floor, CSIS Headquarters, Washington, D.C.

FEATURING

William Barr,

U.S. Attorney General

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James A. Lewis: Well, good morning. Thanks for staying for what's been so far a really good session.

I suppose our next speaker needs no introduction – boy, there's an old one for you. But I will say that William Barr was confirmed as the 85th attorney general by the Senate in February of last year, so it's been almost a year. We are doing this on your anniversary. Great. He's one of only two people in U.S. history to serve twice as attorney general, previously in the George H.W. Bush administration. He was the executive vice president and general counsel for GTE and then Verizon, so very knowledgeable on telecom issues. And prior to serving as attorney – as attorney general he was at one of the law firms here in D.C., one of the big ones.

So without further ado, Mr. Attorney General. (Applause.)

William Barr: Thank you, Jim, and thanks for that introduction. And thank you for hosting this event. Appreciate all of you taking the time to come here and participate. It's good to see so many of my colleagues from the department participating.

You know, my original career goal was to go into the CIA as a China specialist, and therefore I spent six years at Columbia getting a B.A., an M.A. focusing on Chinese studies. And I remember in one of my government classes we were having a debate – and this was in the early '70s – we were having a debate as to which of our foreign adversaries would pose the greatest long-term threat to the United States. And the question was whether it was Russia or China. And I recall the observation of one of my classmates, who was arguing that China posed the greatest long-term challenge to the United States. And he said Russia wants to conquer the world. We can deal with that. China wants to own the world. That's more difficult to deal with. And there's a certain truth in that.

In 1972, our hope was that integrating China into the international economic system would encourage the PRC to liberalize its economy and that a freer market and economic growth would gradually lead to greater political freedom for its citizens. Unfortunately, economic liberalization has only gone so far. While individuals have been permitted some degree of economic freedom, the Communist Party remains in firm control of the economy. It's an architecture of state power whose principal features are central planning, state-owned enterprises, and government subsidies.

Politically, the PRC remains a dictatorship under which the Communist Party elite jealously guard their monopoly on power. Marxist-Leninism and Maoism linger on, primarily as justification for communist rule, which is authoritarian through and through.

The Communist Party is willing to resort to harsh measures to repress any challenge to its one-party rule, whether it is suppressing religion, rounding up and reeducating Uighurs, resisting efforts at self-determination in Hong Kong, or using the great firewall to limit access to ideas and penalize their expression.

For a brief time after the Cold War, we had indulged the illusion of – that democratic capitalism had triumphed and was now unchallenged by any competing ideology. That was a nice – that was nice while it lasted. But we are now in a new era of global tension and competition. And China has emerged as the United States' top geopolitical adversary based on competing political and economic philosophies.

Centuries before communism, China regarded itself as the central kingdom, Zhongguo. And it wasn't central to the region. It was central to the world. And its ambition today is not to be a regional power, but to be a global one.

For China, success is a zero-sum game. In the words of then General Secretary Xi, Communist Party members should concentrate their efforts on building a socialism that is superior to capitalism. Such efforts, Xi claimed, would require party members to concentrate their entire spirit, their entire life, for the socialist ideal. And the reward for this sacrifice would be the eventual demise of capitalism.

I mentioned my classmate's comment about China wanting to own the world, because today I'd like to focus on the challenge of China's drive for economic and technological supremacy. But I'm not suggesting that China's ambitions are merely economic, or that our competition with China is, at bottom, merely an economic rivalry.

The Chinese have long been a commercial people. But for China, purely economic success is not an end in itself. It is a means to a wider political and strategic set of objectives. Throughout its long history, China has always used its economic strength as a tool to achieve its political and strategic objectives.

In 2015, the Chinese leadership launched its Made in China 2025 plan, a sustained, highly coordinated campaign to replace the United States as the dominant technological superpower. The dictatorship has mobilized all elements of Chinese society, all government, all corporations, all academia, and all of its industrious people, to execute seamlessly on an ambitious plan to dominate the core technologies of the future.

This drive is backed by industrial policy involving huge investments in key technologies, massive financing, and subsidies in the hundreds of billions of dollars. Unfortunately, it also involves industrial espionage and theft of technology and intellectual property, as well as forced technology transfers, predatory pricing, leveraging China's foreign direct investment, and strong-arm sales tactics in target markets, including the use of corruption.

Make no mistake about it, China's current technological thrusts pose an unprecedented challenge to the United States. The stakes for our country couldn't be higher. Since the 19th century, the United States has been the world's leaders in innovation and technology. It has been America's technological prowess that has made us prosperous and secure. Our standard of living, our expanding economic opportunities for our young people and for future

generations, and our national security all depend on our continued technological leadership.

In the past, prior administrations and many in the private sector have too often been willing to countenance China's hardball tactics, and it has been this administration that has finally moved to confront and counteract China's playbook. (Applause.)

Today I want to focus on two aspects of the challenge we face. The first is how China jumpstarts its technology initiatives by stealing our technology. And second, I want to explain why China's current focus on dominating 5G technology is of central concern.

The ability of totalitarian countries to engage in central economic planning can at times appear to be an advantage, especially when mobilizing the kind of technological blitzkrieg that we see unfolding today. The downside is that central planning suppresses technological innovation. Breakthrough ideas arise in free societies like ours, which have long led the way in cutting-edge technological development.

The Chinese are trying to have it both ways. While they are orchestrating a centrally planned campaign to dominate key technologies, they are attempting to capture the benefit of our free society by the outright stealing of our technology. The stealing of technology is not a side show; it undergirds and propels their efforts. As my colleague, John Demers, the assistant attorney general for our National Security Division, observed, "China wants the fruits of America's brain power to harvest the seeds of its planned economic dominance."

In 2018, as you've been hearing, the department launched its China Initiative to confront China's maligned behaviors and to protect U.S. technology. As the presentations earlier this morning and throughout the day will demonstrate, investigations during our initiative have repeatedly shown how the PRC is using intelligence services and tradecraft to target valuable scientific and technical information held by the private sector and the academy. This covers a wide range of technologies, from those applicable to commercial airplane engines, to renewable energy, to new materials, to high-tech agriculture.

Since the announcement of Made in China 2025, the Department has brought trade secrets theft cases in eight of the 10 technologies that China is aspiring to dominate. In targeting these sectors, the PRC employs a multi-prong approach, engaging in cyber intrusions, co-opting private sector insiders through its intelligence services, and using non-traditional collectors such as graduate students participating in university research projects.

Chinese theft by hacking has been prominent, and I'm sure you have discussed some of the more recent cases. Those actions by China are continuing, and you should expect more indictments and prosecutions in the future.

Outside cyberspace, defendants pose as U.S. customers to avoid export controls and recruit U.S. employees or co-opt insiders to steal trade secrets. And at academic and other research institutions, China uses talent programs to encourage the theft of intellectual property. And finally, China complements its plainly illicit activities with facially legal but predatory behavior: the acquisition of U.S. companies and other investments in the United States.

The department confronts these threats through the Committee on Foreign Investment in the United States and Team Telecom. As one example, earlier this year, based on a recommendation from the Justice Department and other agencies, the Federal Communications Commission denied a license to China Mobile on national security grounds.

The PRC's economic aggression and theft of intellectual property comes with immense costs. It has been estimated that the annual cost to the U.S. economy could be as high as 600 billion (dollars). The department will continue to use our full suite of national security tools to combat the threat posed by theft directed and encouraged by the PRC. But as I'm sure the – as the FBI director stressed, our ability to protect American technology will ultimately depend on a partnership and working in collaboration with industry and the academy.

Now, let me turn to a very concrete problem that confronts us today. It is the pivotal nature of 5G technology and the threat arising from China's drive to dominate this field.

5G technology lies at the center of the technological and industrial world that is taking shape. In essence, communications networks are not just for communications anymore. They are evolving into the central nervous system of the next generation of internet, the industrial internet, and the next generation of the industrial systems that will depend on that infrastructure.

China has built up a lead in 5G, capturing 40 percent of the global infrastructure market. And for the first time in history, the United States is not leading the next technological era.

Now, much of the discussion on the dangers of allowing China to establish dominance in 5G have been focused on the immediate security concern of using communications networks that China can monitor and surveil. That is, in fact, a monumental danger, and for that reason alone we should mobilize to surmount China's drive to dominate 5G. But the stakes are far higher than this.

It has been estimated that the industrial internet powered by 5G could generate new economic opportunities in the range of 23 trillion (dollars) by 2025. If China establishes sole dominance over 5G, it will be able to dominate the opportunities arising from a stunning range of emerging technologies that will be dependent on and interwoven with the 5G platform.

From a national security standpoint, if the industrial internet becomes dependent on Chinese technology, China would have the ability to shut countries off from

technology and equipment upon which their consumers and industry depend. The power the United States has today to use economic sanctions would pale by comparison to the unprecedented leverage we would be surrendering into the hands of China.

It is important to understand how 5G will enable a revolution in industrial processes. Some Americans think that all we are talking about is analogous to the shift from 3G to 4G in our wireless networks. But we are talking about change that is far more fundamental than merely increasing download speeds for iTunes and websites and movies.

The move from 3G to 4G meant moving from download speeds of about one megabit per second to around 20 megabits per second, and this increase made it possible to move the storage of data and some modest processing power off the devices and onto the cloud. But even this modest evolution of the wireless business spawned wide new fields of innovation, applications, and businesses. And because the United States was the country that developed 4G, we were the country that captured most of the economic opportunity that flowed from that technology.

The jump to 5G is a quantum leap beyond this. We are now talking about multi-gigabyte-per-second peak rates for both download and upload. These fiber-like speeds, coupled with placing Edge computing facilities closer to the users, means 5G is capable of extremely low latency, under 10 milliseconds. And with this capacity, the tiniest devices can have virtually instantaneous connectivity and access the infinite commuting – computing power.

With these characteristics, 5G becomes a real-time, precise system of command and control. Devices of all kinds, some smart, some sensors collecting and transmitting data, some actuators carrying out remote commands, can be dispersed and embedded in business and industrial equipment across a wide array of businesses, such as transportation, energy, finance, health care, agriculture, heavy construction, and so forth. 5G provides the command-and-control function for managing all of these industrial processes.

As the world of 5G unfolds, we will be seeing not just smart homes, smart thermostats, but smart farms, smart factories, smart heavy construction projects, smart transportation systems, and so forth, and a host of new emerging technologies. In addition to artificial intelligence, we'll become interwoven with and dependent on 5G and the industrial internet; for example, robotics, the Internet of Things, autonomous vehicles, 3D printing, nanotechnology, biotechnology, material science, energy storage, and quantum computing.

China has stolen a march, and is now leading in 5G. 5G is an infrastructure business. It relies on radio access network, RAN, facilities. China has two of the leading RAN infrastructure suppliers, Huawei and ZTE. Together, as I've said, they have already captured 40 percent of the market and are aggressively pursuing the balance.

Huawei is now the leading supplier on every continent except North America. The United States does not have an equipment supplier. China's principal competitors are the Finnish firm Nokia, with a 17 percent share, and the Swedish firm Ericsson, with a 14 percent share.

The Chinese are using every lever of power to expand their 5G market share around the globe. It is estimated that a total – the total market for 5G infrastructure is $76 billion. China is offering over $100 billion in incentives to finance customer purchases of its equipment. That means that China can offer its customers to build their 5G networks for no money down. And they have a salesforce and technicians of 50,000 around the globe to push the acceptance of Huawei infrastructure.

In an infrastructure business like 5G – and I say this as someone who spent 15 years in the telecommunications business – scale is critical. The business requires huge investments in R&D, as well as very high capital costs. The larger a company's market share, the better it can afford these costs. Competitors facing a shrinking, addressable market find it harder to sustain the levels of investment required to stay competitive.

Chinese companies start with the advantage of the largest domestic market, giving them instant scale. And as they add this around the world, they will be able to invest more in their technology. The more China gains ground as a supplier of 5G infrastructure, the more it will also gain ground in all the constituent technologies that undergird 5G infrastructure.

5G rests on a stack of technologies, including semiconductors, fiber optics and rare-earth and materials. China has moved to domesticate all of these elements, so it will now – it will not be dependent on foreign suppliers.

Semiconductors provides a good example of the ripple effect of Chinese leadership in 5G. China now consumes over half of the world's semiconductors. China has now started to replace U.S. semiconductors with its own. Its scale in this field will permit it to make the investments needed to close the current quality gap. As China builds its scale in the semiconductor industry, it will place substantial pressure on alternative semiconductor suppliers. And of course, semiconductors are indispensable to a wide range of technology and industries, apart from 5G.

China's success in 5G infrastructure is also translating into advantages in a range of new technologies associated with 5G. Artificial intelligence is a good example. It is interwoven with the industrial internet. As China captures more and more of the data generated by its 5G infrastructure, it can produce better artificial intelligence because that is what artificial intelligence learns from. The more data, the better the AI. It's a virtuous cycle.

Within the next five years, 5G global territory and application dominance will be determined. The question is whether, within this window, the United States and our allies can mount sufficient competition to Huawei to retain and capture

enough market share to sustain the kind of long-term and robust competitive position necessary to avoid surrendering dominance to China. The time is very short, and we and our allies have to act quickly.

While much has to be done, it is imperative to make two decisions right away. First, we have to deploy the spectrum necessary for a robust 5G system in the United States. We haven't done this. This is the mid-band spectrum, called the C-block or the C-band. The FCC has been working hard to get the C-band spectrum out into the market through an auction, and it is critical to get this done within the next very few months. Even then, the United States will need 400,000 base stations to cover the nation if we rely solely on C-band. This could take a decade or more to build out. Just by comparison, today's wireless system runs on 70(,000) to 80,000 base stations. China has already installed approximately 100,000 base stations for 5G. We will have to build 400,000 base stations for nationwide 5G coverage after the C-band is put out.

Now, recently there have been some interesting proposals to jumpstart U.S. 5G by also making available L-band spectrum, for use in tandem with C-band. By using an L-band uplink, we could dramatically reduce the number of base stations required to complete national coverage. It has been suggested that this could cut the time for U.S. 5G deployment from a decade to 18 months and save approximately $80 million. While some technical issues about using the L-band are being debated, it's imperative that the FCC resolve these questions, make its decision on spectrum, and move forward.

The bottom line is that we have to move decisively to auction the C-band and bring resolution on the L-band. Our economic future is at stake. We have to bear in mind in making these spectrum decisions, that given the narrow window we face the risk of losing the 5G struggle with China should vastly outweigh all other considerations.

Second, we have to make a decision on the horse we're going to ride in this race. Who is the 5G equipment supplier or suppliers that we will rely on to compete against Huawei around the globe, to win contracts from operators and blunt Huawei's drive to domination? It's always – it's all very well to tell our friends and allies that they shouldn't install Huawei's, but whose infrastructure are they going to install? If we and our allies, and other countries that do not want to put their economic fate in China's hands are not going to install Huawei's infrastructure, we have to have a market-ready alternative today.

What is a customer looking for, after all? What's the operator looking for in moving from 4G to 5G? It's a one-time decision. It's a big decision. You can't afford to make a mistake. You need to know you are buying a reliable system that will perform, because you don't have the luxury of tearing it out down the road. And, you need a system that will allow you to seamlessly migrate your installed 4G base to 5G. And you need to know that your supplier has staying power – they're not here today and gone tomorrow, they will be there for the long haul.

Those are the products that are necessary to win contracts today, and there are only two companies that can compete with Huawei right now: Nokia and Ericsson. They have the reliable products. They can guarantee performance. They have – they have proven successful in managing customer migration from 4G to 5G. The main concern about these suppliers is that they have neither Huawei's scale nor the backing of a powerful country with a large embedded market, like China.

Now, there have been some proposals that these concerns could be met by the United States aligning itself with Nokia and/or Ericsson through American ownership of a controlling stake, either directly or through a consortium of private American and allied companies. Putting our large market and financial muscle behind one or both of these firms would make it a far more formidable competitor and eliminate concerns over its staying power or their staying power. We and our closet allies certainly need to be actively considering this approach.

Now, recently there has been some talk about trying to develop an OpenRAN approach, which aims to force open the RAN into its components and have those components be developed by U.S. or Western innovators. The problem is that this is a pie in the sky. This approach is completely untested and would take many years to get off the ground, and it would not be ready for primetime for a decade, if ever. What we need today, as I said, was a product that can win contracts right now, a proven infrastructure, one that will blunt Huawei's advance.

As a dictatorship, China can marshal an all-nation approach – the government, its companies, its academia, acting together as one. We're not able to compel this. When we have faced similar challenges in the past, such as World War II and Russia's Cold War technological challenge, as a free people we rallied together. We were able to form a close partnership among government, the private sector, and academia, and through that cooperation we prevailed and the challenges we have met. Unfortunately, the cooperative bonds and sense of purpose we were able to muster in the past are harder to call on today. And in the 1950s, we had the Sputnik moment to help galvanize the nation and bring unity to our response, and we have not seen a similar catalyst today.

If we are going to maintain our technological leadership, our economic strength, and ultimately our national security in the face of this blitzkrieg, we need the public and private sectors to work together and come shoulder-to-shoulder. To our private-sector friends, I would say that appeasing the PRC may come with short-term benefits, but I urge you to question the longstanding assumption that promises of market access are worth the steep costs. The PRC's ultimate goal is to replace you with a Chinese company.

University and think-tank colleagues, I'd ask that you not allow the theft of technology under the guise of academic freedom. Do not allow the PRC to dictate your research or pressure you into ignoring diverse voices on controversial topics. Consider whether any sacrifice of academic integrity or freedom is worth the tradeoff.

And to our allies, I applaud your efforts to stand up to China's economic leverage, but we must do more and act collectively. Let's not forget that our collective economic influence and power is far stronger.

Throughout history, free societies have faced regimented adversaries. At critical junctures they have achieved the unity and purpose necessary to prevail, not because they have been compelled to do so but because they freely choose to do so. We must make that choice today.

Thank you very much. (Applause.)

(END)

An official website of the United States government
Here's how you know

THE UNITED STATES DEPARTMENT of JUSTICE
JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, December 21, 2018

Chinese National Charged with Committing Theft of Trade Secrets

Hongjin Tan, a 35 year old Chinese national and U.S. legal permanent resident, was arrested on Dec. 20 and charged with theft of trade secrets. Tan is alleged to have stolen the trade secrets from his employer, a U.S. petroleum company.

The announcement was made by Assistant Attorney General for National Security John C. Demers, U.S. Attorney Trent Shores for the Northern District of Oklahoma, and Special Agent in Charge Kathryn Peterson of the FBI Oklahoma City Field Office.

"Hongjin Tan allegedly stole trade secrets related to a product worth more than $1 billion from his U.S.-based petroleum company employer, to use for the benefit of a Chinese company where he was offered employment," said Assistant Attorney General Demers. "The theft of intellectual property harms American companies and American workers. As our recent cases show, all too often these thefts involve the Chinese government or Chinese companies. The Department recently launched an initiative to protect our economy from such illegal practices emanating from China, and we continue to make this a top priority."

"The United States filed a criminal complaint against a Chinese national alleging the theft of intellectual property from a company with significant operations in Oklahoma," said U.S. Attorney Shores. "The value of the trade secrets in this case is estimated to be more than $1 billion dollars. Theft of critical research, development, and other intellectual property harms the economic prosperity and security of the United States. My office and the Federal Bureau of Investigation will utilize all tools available to respond to these types of threats. We will protect Oklahomans and Oklahoma businesses by prosecuting those who violate the law."

Tan made an initial appearance Thursday before U.S. Magistrate Judge Jodi F. Jayne. A preliminary and detention hearing has been set for Dec. 26.

According to the criminal complaint, Tan allegedly stole trade secrets from a U.S.-based petroleum company regarding the manufacture of a "research and development downstream energy market product." The company's methods of developing the product are of great value, both economically and to competitors. Until recently, Tan worked for the petroleum company and allegedly downloaded hundreds of files, including files related to the manufacture of the product. Investigators allege that Tan was offered a job at a company in China where he planned to use these files to benefit his new employer. Tan has been residing in the United States for the past 12 years.

A criminal complaint is merely an allegation, and the defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

The FBI conducted this investigation.

Assistant U.S. Attorney Joel-lyn A. McCormick of the Northern District of Oklahoma is prosecuting the case, with assistance from Trial Attorneys Matthew R. Walczewski and Matthew J. McKenzie of the National Security Division's Counterintelligence and Export Control Section (CES) and Assistant Deputy Chief Brian J. Resler of the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS).

Attachment(s):
Download 2018 12 20 Hongjin Tan Complaint

Topic(s):
Counterintelligence and Export Control
National Security

Component(s):
National Security Division (NSD)
USAO - Oklahoma, Northern

Press Release Number:
18-1688

Updated December 21, 2018

An official website of the United States government
Here's how you know

THE UNITED STATES DEPARTMENT of JUSTICE
JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, January 28, 2020

Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases

The Department of Justice announced today that the Chair of Harvard University's Chemistry and Chemical Biology Department and two Chinese nationals have been charged in connection with aiding the People's Republic of China.

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested this morning and charged by criminal complaint with one count of making a materially false, fictitious and fraudulent statement. Lieber will appear this afternoon before Magistrate Judge Marianne B. Bowler in federal court in Boston, Massachusetts.

Yanqing Ye, 29, a Chinese national, was charged in an indictment today with one count each of visa fraud, making false statements, acting as an agent of a foreign government and conspiracy. Ye is currently in China.

Zaosong Zheng, 30, a Chinese national, was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint with attempting to smuggle 21 vials of biological research to China. On Jan. 21, 2020, Zheng was indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. He has been detained since Dec. 30, 2019.

Dr. Charles Lieber

According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities. Unbeknownst to Harvard University beginning in 2011, Lieber became a "Strategic Scientist" at Wuhan University of Technology (WUT) in China and was a contractual participant in China's Thousand Talents Plan from in or about 2012 to 2017. China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure Chinese overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information. Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber $50,000 USD per month, living expenses of up to 1,000,000 Chinese Yuan (approximately $158,000 USD at the time) and awarded him more than $1.5 million to establish a research lab at WUT. In return, Lieber was obligated to work for WUT "not less than nine months a year" by "declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of" WUT.

The complaint alleges that in 2018 and 2019, Lieber lied about his involvement in the Thousand Talents Plan and affiliation with WUT. On or about, April 24, 2018, during an interview with investigators, Lieber stated that he was never asked to participate in the Thousand Talents Program, but he "wasn't sure" how China categorized him. In November 2018, NIH inquired of Harvard whether Lieber had failed to disclose his then-suspected relationship with WUT and

China's Thousand Talents Plan. Lieber caused Harvard to falsely tell NIH that Lieber "had no formal association with WUT" after 2012, that "WUT continued to falsely exaggerate" his involvement with WUT in subsequent years, and that Lieber "is not and has never been a participant in" China's Thousand Talents Plan.

Yanqing Ye

According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China and member of the Chinese Communist Party (CCP). On her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that while studying at Boston University's (BU) Department of Physics, Chemistry and Biomedical Engineering from October 2017 to April 2019, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites and sending U.S. documents and information to China.

According to court documents, on April 20, 2019, federal officers interviewed Ye at Boston's Logan International Airport. During the interview, it is alleged that Ye falsely claimed that she had minimal contact with two NUDT professors who were high-ranking PLA officers. However, a search of Ye's electronic devices demonstrated that at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science. Furthermore, a review of a WeChat conversation revealed that Ye and the other PLA official from NUDT were collaborating on a research paper about a risk assessment model designed to decipher data for military applications. During the interview, Ye admitted that she held the rank of Lieutenant in the PLA and admitted she was a member of the CCP.

Zaosong Zheng

In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. It is alleged that on Dec. 9, 2019, Zheng stole 21 vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. It is alleged that initially, Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

The charge of making false, fictitious and fraudulent statements provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of visa fraud provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of acting as an agent of a foreign government provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. The charge of conspiracy provides for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000. The charge of smuggling goods from the United States provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers, United States Attorney Andrew E. Lelling; Special Agent in Charge of the FBI Boston Field Division Joseph R. Bonavolonta; Michael Denning, Director of Field Operations, U.S. Customs and Border Protection, Boston Field Office; Leigh-Alistair Barzey, Special Agent in Charge of the Defense Criminal Investigative Service, Northeast Field Office; Philip Coyne, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General; and William Higgins, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office made the announcement. Assistant U.S. Attorneys B. Stephanie Siegmann, Jason Casey and Benjamin Tolkoff of Lelling's National Security Unit are prosecuting these cases with the assistance of trial attorneys William Mackie and David Aaron at the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

These case are part of the Department of Justice's China Initiative, which reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

Attachment(s):
Download Download Charging Documents

Topic(s):
Counterintelligence and Export Control
National Security

Component(s):
National Security Division (NSD)
USAO - Massachusetts

Press Release Number:
20-99

Updated January 29, 2020

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of MASSACHUSETTS

U.S. Attorneys » District of Massachusetts » News

Department of Justice

U.S. Attorney's Office

District of Massachusetts

FOR IMMEDIATE RELEASE

Thursday, August 31, 2017

Dual Canadian/Chinese Citizen Arrested for Attempting to Steal Trade Secrets and Computer Information

Defendant allegedly tried to steal next-generation robotics technology

BOSTON – A dual citizen of Canada and China was arrested and charged today in connection with attempting to steal trade secrets and computer information from a Raynham-based medical technology company.

Dong Liu, a/k/a Kevin, 44, was charged in a criminal complaint with one count of attempted theft of trade secrets and one count of attempted access to a computer without authorization and in excess of authorized access with the intent to obtain information from a protected computer. Liu was detained following an initial appearance in federal court in Boston this afternoon.

According to the charging documents, Medrobotics Corporation, which is headquartered in Raynham, Mass., manufactures and markets a unique robot-assisted device that provides surgeons with access to, and visualization of, hard-to-reach places in the human body for minimally invasive surgery. The company has invested millions of dollars in next-generation robotics technology that is not yet patented.

It is alleged that around 7:30 p.m. on Aug. 28, 2017, Medrobotics' CEO spotted a man, later identified as Liu, sitting in a conference room inside the company's secured space with what appeared to be three open laptop computers. He was not a company employee or contractor, so the CEO asked Liu whom he was there to visit. Liu named one company employee whom the CEO knew was out of the country for a few weeks; Liu then identified another employee whom the CEO knew had not scheduled such a meeting; Liu then named the CEO himself, which the CEO knew was not to be true.

Liu allegedly claimed to be working with a Chinese patent law firm. He showed the CEO his LinkedIn biography, in which Liu claimed to lead his firm's intellectual property practice in medical devices, among other things. When police responded to the CEO's call and talked with Liu, Liu gave conflicting explanations about how he had entered the building. A check of Medrobotics' visitor log book revealed that neither Liu nor any other visitor had signed into the building that day, despite a company policy that requires visitors to log in.

According to charging documents, Liu told the CEO that he had entered Medrobotics just before 5:00 p.m. Further investigation revealed that Liu had been seen in the company's lobby taking a video of a monitor displaying public corporate information around 5:00 p.m. and again around 6:00, well before he was discovered in the conference room. The investigation also revealed that Liu had been contacting Medrobotics employees via LinkedIn.

When Liu was arrested by the local police for trespassing, he possessed two laptop computers, an iPad, two portable hard drives, 10 cellphone SIM cards, two digital camcorders, at least two flash drives, and other data equipment. Some of these types of equipment can be used to obtain data from computer networks and to video record otherwise-secret physical documents and products. Further investigation will be required to reveal whether Liu's attempts to obtain computer information or trade secrets were successful.

The charge of attempted theft of trade secrets provides for a sentence of no greater than 10 years in prison, three years of supervised release, and a fine of $250,000, or twice the financial gain or loss, restitution, and forfeiture. The charge of attempted access to a computer to obtain information unlawfully provides for a sentence of no greater than five years in prison, three years of supervised release, and a fine of $250,000, or twice the financial gain or loss, restitution, and forfeiture. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Acting United States Attorney William D. Weinreb; Harold H. Shaw, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Division; Raynham Police Chief James W. Donovan; and Bristol County District Attorney Thomas M. Quinn made the announcement today. Medrobotics cooperated with authorities during the investigation. Assistant U.S. Attorney Scott L. Garland of Weinreb's National Security Unit is prosecuting the case.

The details contained in the complaint are allegations. The defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

Topic(s):
Consumer Protection

Component(s):
USAO - Massachusetts

Updated August 31, 2017

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of MASSACHUSETTS

U.S. Attorneys » District of Massachusetts » News

Department of Justice

U.S. Attorney's Office

District of Massachusetts

FOR IMMEDIATE RELEASE Wednesday, January 27, 2016

Extradited Chinese National Sentenced to Nine Years for Providing U.S. Goods to Iran to Support its Nuclear Program

BOSTON – A Chinese national was sentenced today in U.S. District Court in Boston in connection with supplying a U.S. designated Iranian Weapons of Mass Destruction (WMD) Proliferator with 1,185 pressure transducers that could be used to make nuclear weapons-grade uranium.

Sihai Cheng, a/k/a Chun Hai Cheng, a/k/a Alex Cheng, 35, a citizen of the People's Republic of China (PRC), was sentenced by U.S. District Court Chief Judge Patti B. Saris to nine years in prison. In December 2015, Cheng pleaded guilty to two counts of conspiring to commit export violations and smuggle goods from the United States to Iran and four counts of illegally exporting U.S. manufactured pressure transducers to Iran.

"Cheng knowingly provided more than 1,000 pressure transducers to Iran which advanced its nuclear weapons capabilities," said United States Attorney Carmen M. Ortiz. "At this critical time, the prosecution of individuals who violate our export laws – wherever they are located – is just as important, if not more, than ever before."

"Massachusetts is a worldwide leader of innovative technology and research," said Harold H. Shaw, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Division. "Mr. Cheng smuggled some of that technology used to process weapons-grade uranium into Iran. As this case illustrates, the FBI will do everything it can to keep U.S. weapons technology and other restricted materials from falling into the wrong hands and hurting our nation's security."

"Today's lengthy sentence serves as a warning to others that stiff penalties are waiting for anyone attempting to steal/sell American technologies or trade them to foreign powers," said Matthew Etre, Special Agent in Charge of HSI Boston. "HSI and our law enforcement partners take the national security interests of this nation very seriously and will aggressively pursue any criminal or organization engaged in these activities."

"Today's sentence reaffirms OEE's commitment to identifying, disrupting and enforcing illegal procurement networks and preventing sensitive WMD materials and technology from being exported contrary to U.S. export law," said Michael S. Imbrogna Acting Special Agent in Charge of the Department of Commerce, Office of Export Enforcement, Boston Field Office. "Our special agents will continue to work hand in hand with our law enforcement partners and the U.S. Attorney's Office to protect Americans worldwide."

In 2013, Cheng was charged in an indictment with conspiring to export, and exporting, highly sensitive U.S. manufactured goods with nuclear applications to Iran from at least 2009 to 2012. Cheng pleaded guilty to conspiring with other individuals in China and Iran to illegally obtain hundreds of U.S. manufactured pressure transducers manufactured by MKS Instruments, Inc., a company headquartered in Massachusetts, and export them to Iran. As established at the sentencing hearing, Cheng knew that the parts were being supplied to Kalaye Electric Co., a U.S. designated Iranian WMD Proliferator responsible for the Government of Iran's nuclear centrifuge program and the development of weapons-grade uranium. Pressure transducers can be used in gas centrifuges to enrich uranium and produce weapons-grade uranium and are therefore subject to strict export controls. They cannot be shipped from the United States to China without an export license or shipped from the United States to Iran at all.

At today's sentencing, the government argued that Cheng's conduct gravely harmed and jeopardized the national security of the United States as well as other countries throughout the world. Cheng even invoked the threat of war between Iran and the United States as a means of increasing his profits. Cheng's procurement network was responsible for supplying Iran thousands of components for its nuclear proliferation activities and advancing Iran's nuclear capabilities. Cheng knew he was providing Iran critical components for use in the development of weapons-grade uranium and that the parts he was supplying were going Iran's nuclear program. Indeed, in 2009, according to evidence at the sentencing hearing, when Cheng supplied his first four shipments of pressure transducers, Iran was secretly constructing the Fordow Fuel Enrichment Plant for the purpose of developing nuclear weapons. Further, based upon expert testimony, from 2009 to 2011, when Cheng supplied Iran 1,185 MKS pressure transducers, Iran was engaged in nuclear proliferation activities.

In imposing the nine year sentence, Judge Saris found that Cheng "knowingly provided material support to develop a nuclear weapon."

MKS Instruments, Inc., is not a target of this investigation and has been cooperating in this matter.

U.S. Attorney Ortiz, FBI SAC Shaw, HSI SAC Etre, and Commerce Acting SAC Imbrogna, made the announcement today. Assistance was also provided by the U.S. Department of Energy. The case is being prosecuted by Assistant U.S. Attorney B. Stephanie Siegmann of Ortiz's National Security Unit.

Topic(s):
National Security

Component(s):
USAO - Massachusetts

Updated February 4, 2016

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of MASSACHUSETTS

U.S. Attorneys » District of Massachusetts » News

Department of Justice

U.S. Attorney's Office

District of Massachusetts

FOR IMMEDIATE RELEASE Thursday, May 1, 2014

Woman Sentenced For Illegally Exporting Electronics Components Used In Military Radar, Electronic Warfare And Missile Systems To China

BOSTON – The former manager of a Massachusetts electronics company was re-sentenced yesterday for illegally exporting electronics components to China.

Yufeng Wei, a Chinese national residing in Belmont, Mass., was sentenced to 23 months in prison for conspiring, over a 10 year period, to illegally export military and sophisticated electronics used in military phased array radar, electronic warfare, and missile systems to the People's Republic of China (PRC) and illegally exporting sensitive electronic components to the PRC in violation of the Export Administration Regulations. Several Chinese military entities were among those to whom the defendant and her co-conspirators exported the equipment.

On March 19, 2013, the U.S. Court of Appeals for the First Circuit affirmed Wei's conviction on export violations charges, for which a jury convicted her in May 2010. The First Circuit vacated two counts of the conviction that charged Weiand her now ex-husband, Zhen Zhou Wu, with illegally exporting parts designated on the United States Munitions List because it held that the jury instructions given were constitutionally inadequate. However, the First Circuit observed that, from 1996 until 2008, Wu and Wei, shipped tens of millions of dollars worth of sophisticated electronic components from the United States to China, with little regard for whether the parts that they sold were export-controlled. Further, the First Circuit determined that Wu and Wei repeatedly attempted to disguise the fact that they were exporting to China and that they lacked the necessary licenses to do so. Because two counts of conviction were vacated, the case was remanded for a re-sentencing hearing. Wu was sentenced to 84 months in prison at his re-sentencing hearing held on Sept. 9, 2013.

Wei50, was also sentenced to two years of supervised release. After serving her sentence Wei, who has been residing in the United States as a Lawful Permanent Resident, will be subject to deportation.

On May 17, 2010, WeiWu and Chitron Electronics, Inc. (Chitron-US), were convicted of conspiring from 1997 to 2007 to unlawfully export to the PRC military electronics and export restricted electronics components and illegally exporting such parts to the PRC on numerous occasions between 2004 and 2007. The defendants' illegal enterprise involved the use of Chitron-US, a company Wu established in Waltham, Mass., as a front company for its parent company, Chitron Electronics Company Limited, based in

Shenzhen, PRC. Wei was a "hands-on" manager at Chitron-US who oversaw the procurement of export restricted equipment from U.S. suppliers and shipment of those goods from Waltham to China, through Hong Kong without the suppliers' knowledge. The exported equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment, missile systems, and satellite communications. Many of Chitron's customers were Chinese military research institutes and military entities responsible for procuring, developing, and manufacturing electronic components for China's Army, Navy, and Air Force.

The Department of Defense's Defense Technology Security Administration concluded in a report filed with the Court that the defendants' activities in this case seriously threatened "U.S. national and regional security interests." According to the Department of Defense, the parts the defendants were convicted of illegally exporting are "vital for Chinese military electronic warfare, military radar, fire control, military guidance and control equipment, and satellite communications." The report further concluded that the illegally exported parts are "precisely the [types of] items ... that the People's Liberation Army actively seeks to acquire."

U.S. Attorney Carmen M. Ortiz; Acting Assistant Attorney General John P. Carlin of the Justice Department's National Security Division; John J. McKenna, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office; Bruce Foucart, Special Agent in Charge of Homeland Security Investigations in Boston; Vincent B. Lisi, Special Agent in Charge of the Federal Bureau of Investigation's Boston Field Office; and Leigh-Alistair Barzey, Resident Agent in Charge of Defense Criminal Investigative Service in Boston made the announcement today. The case was prosecuted by Assistant U.S. Attorneys B. Stephanie Siegmann and John A. Capin of Ortiz's Anti-Terrorism and National Security Unit.

Component(s):
USAO - Massachusetts

Updated December 15, 2014

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of MASSACHUSETTS

Department of Justice

U.S. Attorney's Office

District of Massachusetts

FOR IMMEDIATE RELEASE

Tuesday, September 10, 2013

Chinese National Sentenced For Illegally Exporting Military Electronics Components

BOSTON - Zhen Zhou Wu, a Chinese national, was re-sentenced yesterday to 84 months in prison for conspiring over a 10-year-period to illegally export military and sophisticated electronics to the People's Republic of China (PRC).

Wu was also convicted of illegally exporting sensitive electronic components to the PRC on 12 occasions between 2004 and 2007. Several Chinese military entities were among those to whom the defendant exported the equipment, which is used in military phased array radar, electronic warfare, and missile systems. He was also ordered to pay a $15,000 fine. After serving his sentence Wu will be subject to deportation to the PRC.

On March 19, 2013, the U.S. Court of Appeals for the First Circuit affirmed Wu's conviction on 15 of the 17 counts of export violations for which a jury convicted him after a six-week trial in 2010. The First Circuit vacated two counts of conviction that charged Wu with illegally exporting parts designated on the United States Munitions List because it held that the jury instructions given were constitutionally inadequate. However, the First Circuit observed that "from 1996 until 2008, Wu and his co-defendant, Yufeng Wei, shipped tens of millions of dollars worth of sophisticated electronic components from the United States to China, with little regard for whether the parts that they sold were export-controlled." Further, the First Circuit found that Wu's company "specifically pursued military customers; and Wu promoted himself as both an exporter of military supplies and an export compliance expert." Lastly, the First Circuit determined that "Wu and Wei repeatedly attempted to disguise the fact that they were exporting to China and that they lacked the necessary licenses to do so."

Because two counts of the conviction were vacated, the case was remanded for a re-sentencing hearing. Wei's re-sentencing hearing has not yet been scheduled.

On May 17, 2010, Wu, his ex-wife, Wei, and his company, Chitron Electronics, Inc. were convicted of conspiring to unlawfully export to the PRC military electronics from 1997 to 2007 and export restricted electronics components and illegally exporting such parts to the PRC on numerous occasions between 2004 and 2007. The defendants' illegal enterprise involved the use of Chitron Electronics, Inc., a company Wu established in Waltham, Mass., as a front company for its parent company, Chitron Electronics Limited, headquartered in Shenzhen, PRC. Wu used Chitron-US to procure export restricted equipment from US

suppliers and then export the goods to from Waltham to China, through Hong Kong without the suppliers' knowledge. The exported equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment, missile systems, and satellite communications. Many of Chitron's customers were Chinese military research institutes and military entities responsible for procuring, developing, and manufacturing electronic components for China's Army, Navy and Air Force.

The Department of Defense's Defense Technology Security Administration concluded in a report filed with the Court that the defendants' activities in this case seriously threatened "U.S. national and regional security interests." According to the Department of Defense, the parts the defendants were convicted of illegally exporting are "vital for Chinese military electronic warfare, military radar, fire control, military guidance and control equipment, and satellite communications." The report further concluded that the illegally exported parts are "precisely the [types of] items ... that the People's Liberation Army actively seeks to acquire."

United States Attorney Carmen M. Ortiz; Acting Assistant Attorney General John P. Carlin of the Justice Department's National Security Division; John J. McKenna, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office; Bruce Foucart, Special Agent in Charge of Homeland Security Investigations in Boston: Vincent B. Lisi, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Office; and Leigh-Alistair Barzey, Resident Agent in Charge of Defense Criminal Investigative Service in Boston made the announcement. The case is being prosecuted by Assistant U.S. Attorneys B. Stephanie Siegmann and John A. Capin of Ortiz's Anti-Terrorism and National Security Unit.

Component(s):
USAO - Massachusetts

Updated December 15, 2014

United States Department of Justice

PRO IP Act
Annual Report FY 2018

PRO IP ACT ANNUAL REPORT OF THE ATTORNEY GENERAL FY 2018

INTRODUCTION

The Department of Justice (the "Department" or "DOJ")[1] submits this Fiscal Year 2018 ("FY 2018") annual report to the United States Congress pursuant to Section 404 of the *Prioritizing Resources and Organization for Intellectual Property Act of 2008* ("PRO IP Act" or "Act"), Pub. L. No. 110-403. The Act imposes a number of annual reporting requirements on the Attorney General, including actions the Department has taken to implement Title IV of the Act ("Department of Justice Programs") and "a summary of the efforts, activities, and resources the [Department] has allocated to the enforcement, investigation, and prosecution of intellectual property crimes." The Act requires similar reporting by the Director of the Federal Bureau of Investigation ("FBI") on its intellectual property ("IP") enforcement efforts pursuant to Title IV of the Act.

To the extent a particular request seeks information maintained by the FBI, the Department respectfully refers Congress to the FBI Fiscal Year 2018 Report to Congress on Intellectual Property Enforcement ("FBI's Annual Report").

[1] Appendix A contains a glossary of acronyms referenced throughout this report.

Section 404(a) of the PRO IP Act requires the Attorney General to report annually to Congress on the Department's efforts to implement eight specified provisions of Title IV during the prior fiscal year. Those provisions and the Department's efforts to implement them during FY 2018 (*i.e.*, October 1, 2017 through September 30, 2018) are set forth below.

In addition, working closely with the Office of the Intellectual Property Enforcement Coordinator ("IPEC"), the Department contributed to the FY2017-2019 Joint Strategic Plan on Intellectual Property Enforcement, as it did with the 2013 Joint Strategic Plan on Intellectual Property Enforcement (June 2013), the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets (February 2013), the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), and the IPEC's annual reports, among other things. The Department continues to participate in a number of IPEC-led working groups.

(a)(1) State and Local Law Enforcement Grants

> *"(1) With respect to grants issued under Section 401, the number and identity of State and local law enforcement grant applicants, the number of grants issued, the dollar value of each grant, including a breakdown of such value showing how the recipient used the funds, the specific purpose of each grant, and the reports from recipients of the grants on the efficacy of the program supported by the grant. The Department of Justice shall use the information provided by the grant recipients to produce a statement for each individual grant. Such statement shall state whether each grantee has accomplished the purposes of the grant as established in Section 401(b). Those grantees not in compliance with the requirements of this title shall be subject, but not limited to, sanctions as described in the Financial Guide issued by the Office of Justice Programs at the Department of Justice."*

In FY 2018, the Office of Justice Programs ("OJP") awarded grants to support state and local IP law enforcement task forces under the statutory authority of the Department of Justice Appropriations Act 2018, Pub. L. No. 115-141, 132 Stat. 348, 421, and as informed by Section 401 of the PRO IP Act. The Intellectual Property Enforcement Program ("IPEP"), as the grant program is known, is designed to provide national support through training and technical assistance and improve the capacity of state and local criminal justice systems to address criminal IP enforcement, including prosecution, prevention, training, and technical assistance. Under the program, grant recipients establish and maintain effective collaboration and coordination between state and local law enforcement, including prosecutors, multi-jurisdictional task forces, and appropriate federal agencies, including the FBI and United States Attorneys' Offices. The information shared under the program includes information about the investigation, analysis, and prosecution of matters involving IP offenses as they relate to violations of state and local criminal statutes. The program is administered by the Bureau of Justice Assistance ("BJA"), a component of OJP.

In FY 2018, OJP was able to grant seven awards totaling $2,253,259 to local and state law enforcement and prosecutorial agencies. The following FY 2018 new awards cover expenses related to: performing criminal enforcement operations; educating the public to prevent, deter, and identify criminal violations of IP laws; establishing task forces to conduct investigations, forensic analyses, and prosecutions; and acquiring equipment to conduct investigations and forensic analyses of evidence.

Award Number	Grantee	Amount
2018-H2197-CA-IP	City of Los Angeles, California	$400,000.00
2018-H2188-OR-IP	City of Portland, Oregon	$400,000.00
2018-H2178-NC-IP	North Carolina Department of the Secretary of State	$400,000.00
2018-H2198-TX-IP	City of Houston, Texas	$400,000.00
2018-H2080-TX-IP	The City of San Antonio Police Department	$400,000.00
2018-H2179-CA-IP	County of Los Angeles	$400,000.00
2018-H2195-KY-IP	Louisville Metro Government	$24,999.99

Since the inception of the program, OJP has awarded $28,610,772 in grants to support state and local law enforcement agencies, training and technical assistance providers, and an IP public education campaign. Of this total amount of funding, state and local law enforcement agencies have received $21,312,108. Throughout the duration of the program, these agencies have made seizures totaling $675,525,017, which includes counterfeit merchandise and other property valued at $629,053,308, and $16,471,705 in currency.

During a one-year period from July 1, 2017 to June 30, 2018, grantees reported seizures totaling $143,296,457 ($141,902,981 in counterfeit merchandise and other property, and $1,393,476.27 in currency). Over this same one-year period, grantees engaged in the following law enforcement activities:

- 423 individuals were arrested for violations of IP laws;
- 187 state and local IP search warrants were served; and
- 428 piracy/counterfeiting organizations were disrupted or dismantled.

Examples of how state and local law enforcement used prior IPEP grants include:

- After a City of Austin Detective viewed a local news story about counterfeit "Tide" believed to contain dangerous chemicals being sold in five-pound buckets

in the Austin area, the Criminal Conspiracy unit researched and discovered four stores where this counterfeit product was sold. Initially, 188 five-pound gallon buckets were seized, and a distributor was identified. In addition, HSI Dallas seized an additional 125 buckets of the counterfeit "Tide;" police in Los Angeles and Houston also seized counterfeit "Tide."

- The City of Phoenix Police Department's program focused on multiple areas, including money laundering, counterfeit medicine, investment fraud, and cargo theft. The investigators identified supply lines for counterfeit medicine flowing into immigrant communities, targeted seven locations, and seized over 100,000 doses of counterfeit medicine. Several store owners were indicted. Indictments of eight suspects involved in investment fraud and money laundering also are pending. The program also conducted an investigation involving a cargo theft ring consisting of a third party delivery driver for Amazon and his associates. The ring leader used a stolen identity to secure employment at an Amazon fulfillment center; while working at the facility, he stole pallets that were assigned to other drivers. The Phoenix police executed search warrants that resulted in the recovery of tens of thousands of dollars in stolen cargo, and two subjects were indicted.

BJA also continues to support one-day training events on IP rights for state and local law enforcement agencies across the country through cooperative agreements with the National White Collar Crime Center (NW3C). Between July 1, 2017 and June 30, 2018, NW3C conducted these training sessions for 234 attendees from 103 agencies in 8 locations.[2] During this time, NW3C also conducted onsite technical assistance visits for two IPEP Grantee task forces and provided training to 40 students through NW3C's online IP resource in order to improve their investigative and prosecutorial approaches to the problem of IP theft.

Since the inception of the program, BJA has supported the following:

- 104 trainings for 2,404 attendees from 1,246 agencies;
- 16 seminars for 538 attendees from 185 agencies; and
- 33 technical assistance visits for 399 attendees from 118 agencies.

Examples of how attendees utilized the training and technical assistance include:

- An attendee at an NW3C training in San Francisco modeled an investigation after a case example to launch an investigation into area liquor stores selling counterfeit goods. The investigation expanded to certain flea market vendors, and ultimately led to a primary supplier who maintained a local warehouse. A criminal search warrant was served and numerous pallets of thousands of infringing goods valued roughly at $280,000 were seized, as well as $65,000.00 in cash. Federal criminal charges are now pending against the supplier.

[2] Training sessions occurred in Mesa, AZ; Atlanta, GA; Humble, TX; Commerce, CA; Gonzales, LA; Sayreville, NJ; Hartford, CT; and Baton Rouge, LA.

- NW3C recently provided technical assistance to the St. Louis Police Department. This assistance included instruction on writing and properly executing search warrants related to IP theft, as well as direct work with attendees who were preparing to launch several investigations throughout the state. Through this engagement, the St. Louis Police were able to obtain search warrants on numerous targets selling counterfeit goods in the St. Louis area.

(a)(2) Additional Agents of FBI

> *"(2) With respect to the additional agents of the Federal Bureau of Investigation authorized under paragraphs (1) and (2) of section 402(a), the number of investigations and actions in which such agents were engaged, the type of each action, the resolution of each action, and any penalties imposed in each action."*

Please see the FBI's Annual Report, which will be submitted separately pursuant to Section 404(c) of the PRO IP Act.

(a)(3) FBI Training

> *"(3) With respect to the training program authorized under section 402(a)(4), the number of agents of the Federal Bureau of Investigation participating in such program, the elements of the training program, and the subject matters covered by the program."*

Please see the FBI's Annual Report, which will be submitted separately pursuant to Section 404(c) of the PRO IP Act.

(a)(4) Organized Crime Plan

> *"(4) With respect to the organized crime plan authorized under section 402(b), the number of organized crime investigations and prosecutions resulting from such plan."*

As in FY 2009 through FY 2017, Congress did not appropriate funds to support Section 402(b) of the PRO IP Act in FY 2018.[3] Nevertheless, the Department has continued to take a number of actions in an effort to implement this provision. The actions, described below, include (1) increased information sharing and coordination and (2) training and outreach. However, the Department will not be able to provide a specific number of prosecutions directly resulting from these increased efforts for at least two reasons. First, the Department can retrieve statistical information from its database based on the statute charged but not based on the type of defendant or group that committed the offense. Second, it is difficult to determine whether prosecutions involving organized crime groups have resulted directly from these organized crime plan efforts or other ongoing efforts.

In addition to the ongoing activities detailed in PRO IP Act Reports for fiscal years 2009 through 2018, the Department has taken the following additional actions to address this important issue:

Increased Information Sharing and Coordination

The Department, through the Criminal Division, is continuing to coordinate with federal investigatory agencies to work with the International Organized Crime Intelligence and Operations Center in an ongoing effort to develop and implement a mechanism to both contribute data to the Center to address intelligence gaps as they relate to IP, among other things. The Center has provided operational, intelligence, and financial support to investigations where international organized crime groups are involved in IP offenses.

Training and Outreach

In FY 2018, the Computer Crime and Intellectual Property Section ("CCIPS") of the DOJ's Criminal Division has continued to strengthen the Department's ability to combat organized IP crime through training and outreach with international counterparts and organizations, which often encounter IP crime committed by organized crime groups. These training and outreach activities are described in section (a)(7)(B) of this Report.

Executive Order

On February 9, 2017, President Trump issued an Executive Order on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International

[3] Section 402(b) provides that "[s]ubject to the availability of appropriations to carry out this subsection, and not later than 180 days after the date of the enactment of this Act, the Attorney General, through the United States Attorneys' Offices, the Computer Crime and Intellectual Property section, and the Organized Crime and Racketeering section of the Department of Justice, and in consultation with the Federal Bureau of Investigation and other Federal law enforcement agencies, such as the Department of Homeland Security, shall create and implement a comprehensive, long-range plan to investigate and prosecute international organized crime syndicates engaging in or supporting crimes relating to the theft of intellectual property."

Trafficking. DOJ is working together in partnership with the Department of State, Department of Homeland Security, and the Office of the Director of National Intelligence to implement Executive Order 13773. As part of this implementation, DOJ will continue to address the links between transnational criminal organizations and IP crime.

(a)(5) Authorized Funds Under Section 403

> *"(5) With respect to the authorizations under section 403—*
>
> *(A) the number of law enforcement officers hired and the number trained;*
> *(B) the number and type of investigations and prosecutions resulting from the hiring and training of such law enforcement officers;*
> *(C) the defendants involved in any such prosecutions;*
> *(D) any penalties imposed in each such successful prosecution;*
> *(E) the advanced tools of forensic science procured to investigate, prosecute, and study computer hacking or intellectual property crimes; and*
> *(F) the number and type of investigations and prosecutions in which such tools were used."*

Section 403 related to funds appropriated during FY 2009-2013. No funds were appropriated under this section or expended during FY 2018 based on funds previously appropriated under this section. Information about the cases, defendants, and types of investigations carried out by the Department may be found in greater detail below.

Please see the FBI's Annual Report, provided separately under Section 404(c) of the PRO IP Act, for details on FBI allocation of resources.

(a)(6) Other Relevant Information

The Department did not receive any authorizations under Sections 402 and 403 of the PRO IP Act in FY 2018.

(a)(7) Efforts, Activities and Resources Allocated to the Enforcement of IP Crimes

> *"(6) Any other information that the Attorney General may consider relevant to inform Congress on the effective use of the resources authorized under sections 401, 402, and 403."*

"(7) A summary of the efforts, activities, and resources the Department of Justice has allocated to the enforcement, investigation, and prosecution of intellectual property crimes, including –

(A) a review of the policies and efforts of the Department of Justice related to the prevention and investigation of intellectual property crimes, including efforts at the Office of Justice Programs, the Criminal Division of the Department of Justice, the Executive Office of United States Attorneys, the Office of the Attorney General, the Office of the Deputy Attorney General, the Office of Legal Policy, and any other agency or bureau of the Department of Justice whose activities relate to intellectual property;

(B) a summary of the overall successes and failures of such policies and efforts;

(C) a review of the investigative and prosecution activity of the Department of Justice with respect to intellectual property crimes, including –

(i) the number of investigations initiated related to such crimes;
(ii) the number of arrests related to such crimes; and
(iii) the number of prosecutions for such crimes, including—

(I) the number of defendants involved in such prosecutions;
(II) whether the prosecution resulted in a conviction; and
(III) the sentence and the statutory maximum for such crime, as well as the average sentence imposed for such crime; and

(D) a Department-wide assessment of the staff, financial resources, and other resources (such as time, technology, and training) devoted to the enforcement, investigation, and prosecution of intellectual property crimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting intellectual property crimes."

(a)(7)(A) Review of the Department's Policies and Efforts Relating to the Prevention and Investigation of IP Crimes

The Department investigates and prosecutes a wide range of IP crimes, including those involving copyrighted works, trademarks, and trade secrets. Primary investigative and prosecutorial responsibility within the Department rests with the FBI, the United States Attorneys' Offices, CCIPS in the Criminal Division, the Counterintelligence and Export Control Section ("CES") in the National Security Division ("NSD"), and, with regard to offenses arising under the Food, Drug, and Cosmetic Act, the Consumer Protection Branch of the Civil Division. Each of these components is described briefly below.

In addition to enforcing existing criminal laws protecting IP, the Department has continued its tradition of contributing to major legislative developments updating criminal IP laws, including: the Defend Trade Secrets Act of 2016, which was notable not only for creating a federal civil cause of action for misappropriation of trade secrets, but also increased criminal fines for organizational defendants who steal commercial trade secrets, and allowed prosecutors to bring racketeering charges based on the theft of trade secrets; the Foreign and Economic Espionage Penalty Enhancement Act of 2012, which increased fines for theft of trade secrets committed with the intent to benefit a foreign entity; the Theft of Trade Secrets Clarification Act of 2012, which clarified that the Economic Espionage Act applies to trade secrets that are "related to a product or service used or intended for use in interstate or foreign commerce"; the National Defense Authorization Act for FY 2012, which enhanced penalties for certain offenses involving counterfeit military goods; the Food and Drug Administration Safety and Innovation Act, which created a new offense for trafficking in counterfeit drugs; the PRO IP Act of 2008; the Family Entertainment and Copyright Act of 2005, which criminalized "camcording" (the illegal copying of movies in a theater) and unauthorized distribution of pre-release works over the Internet; the No Electronic Theft Act of 1997, which criminalized the unauthorized reproduction and distribution of copyrighted works even without a commercial purpose or financial gain; and the Economic Espionage Act of 1996, which criminalized the theft of trade secrets, including economic espionage.[4]

The Department made substantial contributions to the criminal enforcement proposals contained in the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations (March 2011), the majority of which (described above) were enacted into law, with the exception of felony penalties for copyright infringement by online streaming. The Department looks forward to working with Congress as it considers additional proposals.

The Department coordinates closely with IPEC in addressing the Administration's priorities on IP enforcement and implementing the IPEC's FY2017-2019 Joint Strategic Plan ("JSP") on Intellectual Property Enforcement. As part of the JSP implementation, the Department participates in a variety of interagency working groups designed to address topics including engagement with private stakeholders; money laundering / criminal financing; engagement with other countries; domestic application of the "Whole of Government" and "Specialized Office" approaches to IPR protection and enforcement; storage, destruction, and disposal of seized counterfeit goods; trade secrets / cybersecurity; and advancing the JSP's "Calls for Research."

CCIPS and CHIP Program

The Department carries out its overall IP criminal prosecution mission through the United States Attorneys' Offices and CCIPS, which works closely with a network of over 270 specially-

[4] For an overview of the Department's policies and efforts in the five years prior to the enactment of the PRO IP Act in October 2008, the Department's PRO IP Act First Annual Report 2008-2009 may be found online at https://www.justice.gov/iptf/pro-ip-act-reports. The Department's FY 2010-FY 2016 PRO IP Reports are available at the same location.

trained federal prosecutors who make up the Department's Computer Hacking and Intellectual Property ("CHIP") program.

CCIPS is a section within the Criminal Division consisting of a specialized team of forty prosecutors who are devoted to enforcing laws related to computer and IP crimes. Fifteen CCIPS attorneys are assigned exclusively to IP enforcement. These attorneys prosecute criminal cases, assist prosecutors and investigative agents in the field, and help develop and implement the Department's overall IP enforcement strategy and legislative priorities. CCIPS attorneys are available to provide advice and guidance to agents and prosecutors on a 24/7 basis. CCIPS attorneys also provide training on criminal enforcement of IP laws to prosecutors and investigative agents both domestically and abroad.

CCIPS also houses the Cybercrime Lab, which provides support in evaluating digital evidence in IP cases. The Lab is currently staffed with nine computer forensics experts. In addition to evaluating digital evidence, the Lab's experts have provided extensive training on the use of digital forensics tools in IP cases to law enforcement audiences around the world.

CCIPS continues to place a high priority on fostering international cooperation and coordination of criminal IP enforcement efforts. The Section has developed relationships with foreign law enforcement through international casework as well as through training and outreach. An important component of the Department's international enforcement efforts is the Intellectual Property Law Enforcement Coordinator ("IPLEC") program. Through the current program, the Department has had an experienced federal prosecutor in Bangkok, Thailand, to coordinate law enforcement activities in Asia since 2006. The IPLEC program has continued to expand, and with the assistance of the State Department, the DOJ has posted regional IPLECs in Bucharest, Romania; Hong Kong; Sao Paolo, Brazil; and Abuja, Nigeria.

The CHIP program is a network of experienced and specially-trained federal prosecutors who aggressively pursue computer crime and IP offenses. Each of the 94 United States Attorneys' Offices has one or more CHIP coordinator. In addition, 25 United States Attorneys' Offices have CHIP Units, with two or more CHIP attorneys.[5] CHIP attorneys have four major areas of responsibility including: (1) prosecuting computer crime and IP offenses; (2) serving as the district's legal counsel on matters relating to those offenses and the collection of electronic evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities.

[5] CHIP Units are currently located in Alexandria, Virginia; Atlanta, Georgia; Austin, Texas; Baltimore, Maryland; Boston, Massachusetts; Brooklyn, New York; Chicago, Illinois; Dallas, Texas; Denver, Colorado; Detroit, Michigan; Kansas City, Missouri; Los Angeles, California; Miami, Florida; Nashville, Tennessee; Newark, New Jersey; New Haven, Connecticut; New York, New York; Orlando, Florida; Philadelphia, Pennsylvania; Pittsburgh, Pennsylvania; Sacramento, California; San Diego, California; San Jose, California; Seattle, Washington; and Washington, D.C.

CES and the NSCS Network

Within NSD, CES—one of NSD's principal litigating components—is responsible for coordinating and conducting investigations and prosecutions of a wide variety of national security offenses, including economic espionage.[6] In June 2015, NSD, recognizing the increasingly acute and costly threat that economic espionage poses to the U.S. national and economic security, released its "Strategic Plan for Countering the Economic Espionage Threat." This plan aims to heighten awareness of the threat in order to deter and mitigate economic espionage. The plan also seeks to coordinate efforts within the government to counter the threat, including through operational disruption, increased and improved training, and the provision of technical advice and expertise. In January 2017, CES released its "Strategic Plan for Countering the National Security Cyber Threat," which recognizes that our nation's adversaries are also stealing intellectual property through cyber-enabled means and proposes a strategy specifically designed to disrupt such efforts. NSD is currently in the process of implementing both plans.

In 2012, the Department established the National Security Cyber Specialists ("NSCS") Network to create a "one-stop-shop" for attorneys, investigators, and members of the private sector looking to combat national security cyber thefts—including economic espionage and trade secret theft—with all appropriate legal tools. Each U.S. Attorney's Office has at least one representative to the NSCS Network, and in each of the last six years NSCS Network representatives have convened in the D.C. area for specialized training focusing on legal and other issues at the intersection of national security and cybersecurity. The NSCS representative provides technical and specialized assistance to his or her colleagues within the relevant U.S. Attorney's Office, and serves as a point of contact for coordination with the Department's headquarters. At headquarters, all NSD components, CCIPS, and other relevant sections of the Criminal Division are members of the Network. The Department relies on the NSCS Network to disseminate intelligence and other information to the field, to train prosecutors on investigating national security cybercrimes, and to coordinate and de-conflict national security cyber investigations.

Interagency Coordination

In addition to investigating and prosecuting IP crime, the Department has worked closely with other federal agencies directly, and through the National Intellectual Property Rights Coordination Center ("IPR Center"), to improve IP enforcement domestically and overseas.[7]

---

[6] In 2015, CES changed its name from the "Counterespionage Section" to better reflect the scope of its work.

[7] These federal agencies include Customs and Border Protection ("CBP"), the Federal Bureau of Investigation ("FBI"), the United States Postal Inspection Service, the Food and Drug Administration's Office of Criminal Investigations, the Department of Commerce's International Trade Administration, the Naval Criminal Investigative Service, the Defense Criminal Investigative Service, the Defense Logistics Agency's Office of Inspector General, Immigration and Customs Enforcement's Homeland Security Investigations ("ICE-HSI"), the United States Nuclear Regulatory Commission, the United States Patent and Trademark Office ("USPTO"), the General Service Administration's Office of Inspector General, the

These activities have included training investigators and prosecutors in the investigation and prosecution of IP crimes; contributing to the Office of the United States Trade Representative's Special 301 process of evaluating the adequacy of our trading partners' criminal IP laws and enforcement regimes; helping to catalogue and review the United States government's IP training programs abroad; and implementing an aggressive international program to promote cooperative enforcement efforts with our trading partners and to improve substantive laws and enforcement regimes in other countries.

(a)(7)(B) Summary of Overall Successes and Failures of Such Policies and Efforts

The Department achieved notable success in FY 2018 both domestically and abroad. Some of these efforts are highlighted below:

Prosecution Initiatives

The Department continues to prioritize IP investigations and prosecutions that involve (1) health and safety, (2) trade secret theft or economic espionage, and (3) large-scale commercial counterfeiting and online piracy. The Department has also increased its focus on IP crimes that are committed or facilitated by use of the Internet or perpetrated by organized criminal networks.

(1) Health and Safety

The Department's health and safety initiative brings together private, state, and federal enforcement resources to address the proliferation of counterfeit goods posing a danger to consumers, including counterfeit and illegally prescribed pharmaceuticals, automotive parts, and military goods. In FY 2018, this initiative resulted in a number of significant prosecutions, including those set forth below:

- *Defendant Sentenced To Prison For Selling Counterfeit Airbags.* On October 4, 2017, Vitaliy Fedorchuk was sentenced to one year and one day in prison and a $5,000 fine for an international scheme to sell counterfeit airbags via eBay and other internet sales sites. Fedorchuk had pleaded guilty on May 31, 2017, to five counts of mail fraud. Between June 23, 2014, and July 27, 2016, Fedorchuk offered for sale airbag modules, covers, and manufacturer emblems at his eBay online store, redbarnautoparts. Fedorchuk falsely advertised that the counterfeit airbags were original equipment from major automobile manufacturers such as Honda, Fiat, Chrysler, Nissan, Toyota, GMC and Ford.

- *Drug Dealer Charged In Manhattan Federal Court For Selling Heroin And Counterfeit Oxycodone Over The Internet.* On October 23, 2017, Cristian Rodriguez was arrested and charged with one count of distributing and possessing with intent to distribute heroin and

---

Consumer Product Safety Commission, the National Aeronautics and Space Administration's Office of Inspector General, the Department of State's Office of International Intellectual Property Enforcement, the Army Criminal Investigation Command's Major Procurement Fraud Unit, the Air Force Office of Special Investigations, the U.S. Postal Service Office of Inspector General, and the Federal Maritime Commission.

oxycodone. Since at least May 2016, Rodriguez and his co-conspirators anonymously sold and distributed controlled substances over the Internet via online marketplaces and "dark web" sites. Rodriguez shipped various prescription drugs, including counterfeit oxycodone, which was actually made of heroin and other substances, to individuals across the United States.

- *Dominican National Arrested and Charged with Fentanyl Conspiracy Including the Distribution of Counterfeit Pain Pills.* On December 20, 2017, Santiago Pena was charged with conspiracy to distribute 40 grams or more of fentanyl. The charge stems from Pena's participation in a large-scale fentanyl and heroin trafficking ring that was dismantled in August 2017. Pena is the seventh defendant related to the drug trafficking operation to be charged in federal court; approximately 10 other defendants have been charged in state court. A lengthy wiretap investigation revealed that James Ramirez, an individual charged separately, supplied large-quantities of fentanyl and heroin to drug dealers on Cape Cod. According to the indictment, Pena brokered fentanyl pill deals on Ramirez's behalf, helping to connect Ramirez with a fentanyl pill supplier. Pena pleaded guilty on March 19, 2018, and is scheduled to be sentenced on November 27, 2018.

- *Three Individuals Sentenced for Operating an Illegal Steroid and Counterfeit Prescription Drug Lab.* On February 1, 2018, Ryan Anthony Sikora was sentenced to 41 months in prison, Ariel Anna Murphy was sentenced to 12 months, and John Joseph Bush, II was sentenced to 8 months for their involvement in a steroid and counterfeit prescription drug lab in Northwest Florida. The three received their sentences after pleading guilty to conspiracy charges for importing, manufacturing, and distributing anabolic steroids as well as counterfeit prescription drugs. The investigation began when U.S. Postal Inspectors determined that large amounts of steroid and counterfeit prescription drug ingredients were being shipped from China to various locations in South Alabama and Northwest Florida. They marketed the counterfeit drugs online using the brand name "Future Pharma" and they would typically process the orders through encrypted email, and then use the U.S. Postal Service to send the contraband products across the United States.

- *Four Individuals Indicted For Trafficking In Counterfeit Goods.* On March 7, 2018, Carlos Enrique Velázquez-Gines, Mayra Evelise Gines-Otero, Noriam Ivette Flores-Deleon, and Vanessa Marrero-Hernández, were charged with mail and wire fraud conspiracy, mail fraud, trafficking in counterfeit goods, introducing misbranded articles into interstate commerce, distribution of a controlled substance, international money laundering, and smuggling. According to the indictment, from at least on or about October 3, 2013, defendants purchased from overseas suppliers located in China, and imported into the United States, dietary supplements, latex condoms, and cosmetics that were counterfeit and/or misbranded under the Federal Food, Drug, and Cosmetic Act. Defendants marketed and sold the products through "online stores" on platforms such as eBay.com and Bonanzo.com. Marrero-Hernández pleaded guilty on October 2, 2018, and Flores-Deleon pleaded guilty on October 18, 2018. The trial for Velazquez-Gines and Gines-Otero is scheduled to being on December 4, 2018.

- *Six Massachusetts Defendants Sentenced for Roles in Counterfeit Steroid Conspiracy.* On March 15, 2018, Tyler Baumann was sentenced to 120 months incarceration; on March 15, 2018, Kathryn Green was sentenced to 1 year and 1 day incarceration; on March 30, 2018, Phillip Goodwin was sentenced to 130 months incarceration; on April 25, 2018, Melissa Sclafani was sentenced to 1 year and 1 day incarceration; on June 20, 2018, Brian Petzke was sentenced to 2 years incarceration and 2 years of supervised release; and on June 20, 2018, Elizabeth Green was sentenced to 2 years of probation. Baumann and Goodwin pleaded guilty to various offenses, including trafficking in counterfeit drugs. Kathryn Green pleaded guilty to one count of conspiracy to distribute controlled substances. Sclafani pleaded guilty to conspiracy to distribute counterfeit steroids. Petzke and Elizabeth Green pleaded guilty one count of conspiracy to distribute controlled substances. From approximately May 2015 until April 12, 2017, the defendants manufactured steroid products made from raw materials that they purchased overseas and marketed as "Onyx" steroids using "Onyx" labels that were also ordered from overseas suppliers. Onyx, now owned by Amgen Inc., is a legitimate pharmaceutical company that does not manufacture steroids. The defendants sold the steroids to customers across the United States using email and social media platforms, collected payment through money remitters, such as Western Union and MoneyGram, and used false identifications and multiple remitter locations to pick up the proceeds.

- *Canadian Pharmacist Sentenced for Distributing Counterfeit and Adulterated Botox to Local Doctors.* On April 4, 2018, Nikhil Buhecha pleaded guilty and was sentenced to 36 months' imprisonment for conspiring to distribute counterfeit, misbranded, and adulterated Botox® into the United States, including multiple shipments to two doctors located in St. Louis County, Missouri. Buhecha owned and operated a sophisticated wholesale drug distribution business involving multiple persons in Canada, Panama, and Turkey. Buhecha sourced Botox® from Turkey and shipped it to multiple U.S. doctors in Missouri and other states. The FDA issued several public safety alerts about these events.

- *Mexican Nationals Plead Guilty to Trafficking in Counterfeit Goods by Operating Counterfeit Airbag Business in Albuquerque.* On May 9, 2018, Two Mexican nationals entered guilty pleas to operating a counterfeit airbag business out of their residence in Albuquerque, New Mexico. Dina Gonzalez-Marquez and Emilio Gonzalez-Marquez, conspired to traffic in counterfeit goods from January 2015 to March 2017, by operating a business that sold counterfeit airbag modules and airbag covers out of their Albuquerque residence. They facilitated the conspiracy by listing and selling counterfeit airbag modules and airbag covers online, shipping the counterfeit goods to purchasers, and conducting in person sales of the counterfeit goods.

- *South Carolina Couple Sentenced to a Total of 138 Months in Prison for Trafficking Counterfeit Goods, Including Misbranded Pet Medicine.* On May 9, 2018, David Haisten and Judy Haisten were sentenced to 78 and 60 months of incarceration, respectively. A jury found the Haistens guilty in October 2017 of conspiracy as well as six counts of violating the Federal Insecticide, Fungicide, and Rodenticide Act, five counts of distributing misbranded animal drugs, and two counts of trafficking in counterfeit goods.

The defendants' products, including pesticides that are extremely toxic in the wrong dose, posed a serious risk to animals and humans.

- *Long Beach Man Sentenced to Over 26 Years in Prison for Leading Counterfeit Opioid Scheme that Distributed Fentanyl Analogue.* On July 9, 2018, Gary Resnik was sentenced to 320 months in federal prison. Resnik was the leader of a narcotics distribution ring that imported a powerful fentanyl analogue from China and produced hundreds of thousands of opioid pills that were distributed in bulk across the nation. Resnik pleaded guilty in August 2017 to two felony offenses—conspiracy to manufacture and distribute narcotics (including acetylfentanyl and ecstasy), and possession with the intent to distribute acetylfentanyl. Resnik admitted to importing from China bulk chemicals, including acetylfentanyl, that were used to manufacture opioid pills. His drug organization also illegally imported pill presses from China that were used to make pills in homemade labs in a Long Beach storage unit and Baldwin Park house. A co-defendant in this case – Christopher Bowen, of downtown Los Angeles – was sentenced in May 2018, to 320 months in federal prison for participating in the drug-trafficking conspiracy.

- *Two Indicted for Trafficking Counterfeit Oxycodone Pills Containing Fentanyl.* On July 19, 2018, Alfredo Sanchez of Madera, and Saybyn Borges, of Sacramento, were indicted on charges relating to their scheme to distribute counterfeit oxycodone pills that contained Fentanyl. Specifically, the defendants were charged with conspiracy to distribute fentanyl, distribution of fentanyl, possession with intent to distribute fentanyl, and being a felon in possession of a firearm. According to other court filings, Sanchez and Borges were involved in the sale of approximately 7,500 counterfeit oxycodone pills that contained fentanyl, a synthetic opioid.

- *Cheektowaga Man Pleads Guilty to Buying and Selling Counterfeit Airbags.* On August 30, 2018, Raymond Whelan pleaded guilty to conspiracy to traffic in counterfeit goods and is scheduled to be sentenced on December 17, 2018. Between June 2015 and March 2016, Whelan and co-defendant David Nichols entered into an agreement to sell counterfeit automobile airbags. Whelan would contact Nichols and order numerous airbags bearing counterfeit trademarks of Honda, Toyota, Nissan, Subaru, Mazda, Hyundai, Acura, and Mitsubishi. Nichols would then locate manufacturers in China to supply the requested airbags. In order to avoid detection during importation, the airbags were purposefully mislabeled. Once imported into the United States, Whelan would sell the airbags as genuine used airbags on eBay utilizing the name Rayscarparts71. Co-defendant David Nichols was previously convicted, and is scheduled to be sentenced on January 31, 2019.

(2) Protecting American Business from Commercial and State-Sponsored Trade Secret Theft

In FY 2018, Department prosecutors and the FBI have continued to emphasize the investigation and prosecution of commercial and state-sponsored trade secret theft. This

continuing focus has led to the investigation and prosecution of numerous trade secret thefts and economic espionage cases. Recent cases include:

- *Three Chinese Hackers Charged Firm for Hacking Three Corporations for Commercial Advantage.* On November 27, 2017, Chinese nationals Wu Yingzhuo, Dong Hao and Xia Lei were indicted for computer hacking, theft of trade secrets, conspiracy and identity theft directed at U.S. and foreign employees and computers of three corporate victims in the financial, engineering and technology industries between 2011 and May 2017. The three Chinese hackers work for the purported China-based Internet security firm Guangzhou Bo Yu Information Technology Company Limited (a/k/a "Boyusec"). The indictment alleges that the defendants conspired to hack into private corporate entities in order to maintain unauthorized access to, and steal sensitive internal documents and communications from, those entities' computers. For one victim, information that the defendants targeted and stole between December 2015 and March 2016 contained trade secrets.

- *Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret From U.S. Company.* On January 17, 2018, Jiaqiang Xu was sentenced to 5 years in prison after pleading guilty to theft of trade secrets and economic espionage on May 19, 2017. The six-count indictment returned in June 2016 alleged that Xu stole proprietary source code from a former employer with the intent to benefit the National Health and Family Planning Commission of the People's Republic of China. From November 2010 to May 2014, Xu worked as a developer and was granted access to proprietary software and its underlying source code. In May 2014, Xu voluntarily resigned and subsequently communicated with undercover law enforcement officer that he had experience with his former employer's proprietary software and proprietary source code. As a result of the communications, Xu uploaded a functioning copy of the proprietary software to an undercover computer network.

- *Chinese Intelligence Officer Charged with Economic Espionage and Theft of Trade Secrets from Leading U.S. Aviation Companies.* On April 1, 2018 a Chinese Ministry of State Security (MSS) operative, Yanjun Xu was arrested in Belgium, pursuant to a federal complaint, and then indicted by a federal grand jury in the Southern District of Ohio. The four-count indictment charges Xu with conspiring and attempting to commit economic espionage and theft of aviation trade secrets. Xu was extradited to the United States on October 9, 2018.

- *Two Businessmen Charged With Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company.* On April 26, 2018, Shan Shi and Gang Liu were charged with conspiracy to commit economic espionage for the benefit of CBM-Future New Material Science and Technology Co. Ltd. (CBMF), a Chinese company based in Taizhou. Both businessmen were previously indicted in June 2017 for conspiracy to commit theft of trade secrets. According to court records, Shi and Liu conspired with others to commit economic espionage and steal trade secrets from a U.S. engineering firm that produces syntactic foam, a strong, lightweight material with commercial and military uses. Shan, Liu, Uka Kalu Uche, Samuel Abotar Ogoe, Kui Bo, and Hui Huang

were indicted in June 2017 on a charge of conspiracy to commit theft of trade secrets. An additional defendant pleaded guilty to the charge in December 2017. The superseding indictment includes that charge, adds the conspiracy to commit economic espionage count against Shi and Liu, and includes a federal money laundering conspiracy count against Shi. Uche pleaded guilty on April 27, 2018, and was sentenced on August 10, 2018 to 12 months probation. Ogoe pleaded guilty on October 17, 2018.

- *Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets.* On July 6, 2018, a manufacturer and exporter of wind turbines based in the People's Republic of China was sentenced for stealing trade secrets from AMSC, a U.S.-based company formerly known as American Superconductor Inc. The Court found that AMSC's losses from the theft exceeded $550 million, and imposed the maximum statutory fine in the amount of $1.5 million on Sinovel Wind Group LLC. Sinovel was convicted of conspiracy to commit trade secret theft, theft of trade secrets, and wire fraud on January 24, 2018 following a jury trial.

- *Electrical Engineer Found Guilty for Intending to Convert Trade Secrets from Defense Contractor.* On July 9, 2018, Jared Dylan Sparks was found guilty for his conduct related to a scheme to convert trade secrets belonging to a defense contractor, related to, among others, an innovative naval prototype being developed for the U.S. Navy. The jury found Sparks guilty of six counts of theft of trade secrets, six counts of uploading trade secrets, and one count of transmitting trade secrets. According to evidence admitted at trial, Sparks, an electrical engineer, worked at LBI Inc., a defense contractor that designs and builds unmanned underwater vehicles for the U.S. Navy's Office of Naval Research and deployable ice buoys for the National Oceanic and Atmospheric Administration. Before he left LBI, Sparks surreptitiously uploaded thousands of LBI files to his personal account with Dropbox, a cloud-based file-storage application.

- *Former DuPont Employee Pleads Guilty to Stealing Trade Secrets and Lying to the FBI.* On July 11, 2018, Josh Harry Isler pleaded guilty to one count of trade secret theft and one count of making a false statement or representation to the FBI. As part of his guilty plea, Isler admitted that during August 2013, while employed with DuPont, but after having accepted an offer of employment from a competitor, he stole trade secrets of DuPont. In a plea agreement, Isler admitted that after he accepted employment with a competitor of DuPont in the ethanol fuel enzyme business, he transferred hundreds of DuPont's electronic files to an external device. Isler also admitted that when he was interviewed by the FBI in November 2013, he falsely denied he had downloaded files containing proprietary information.

- *Former Apple Employee Indicted On Theft of Trade Secrets.* On July 12, 2018, Xiaolang Zhang was indicted for theft of trade secrets. According to the Indictment, Zhang is alleged to have taken a confidential 25-page document containing detailed schematic drawings of a circuit board designed to be used in the critical infrastructure of a portion of an autonomous vehicle, knowing that the theft would injure the owner of the trade secrets, Apple, Inc. Court documents filed allege that on April 30, 2018, Zhang told Apple personnel that he was resigning from his job so that he could return to China to be

closer to his mother who was ill. Apple subsequently learned that Zhang went to work for X-MOTORS—a company focused on electric automobiles and autonomous vehicle technology with its headquarters in China. On July 7, 2018, FBI Agents learned that Zhang purchased a last-minute round-trip airline ticket with no co-travelers, departing for Hangzhou, China aboard Hainan Airlines. Federal agents intercepted and arrested Zhang at the San Jose International Airport after he had passed through the security checkpoint.

- *New York Man Charged With Theft of Trade Secrets.* On August 1, 2018, Xiaoqing Zheng was arrested in connection with a criminal complaint charging him with stealing trade secrets belonging to General Electric (GE). The criminal complaint alleges that on or about July 5, Zheng, an engineer employed by GE, used an elaborate and sophisticated means to remove electronic files containing GE's trade secrets involving its turbine technologies. Specifically, Zheng is alleged to have used steganography to hide data files belonging to GE into an innocuous looking digital picture of a sunset, and then to have e-mailed the digital picture, which contained the stolen GE data files, to Zheng's e-mail account.

- *Second Former GlaxoSmithKline Scientist Pleads Guilty to Stealing Trade Secrets to Benefit Chinese Pharmaceutical Company.* On September 14, 2018, Dr. Tao Li pleaded guilty to conspiracy to steal trade secrets from GlaxoSmithKline (GSK) for the benefit of a Chinese pharmaceutical company named Renopharma. Dr. Li and two of his friends, Dr. Yu Xue and Dr. Yan Mei, created Renopharma in Nanjing, China, supposedly to research and develop anti-cancer drugs. In reality, Renopharma was used as a repository of stolen information from GSK. The data contained information regarding multiple biopharmaceutical products under development, GSK research data, and GSK processes regarding the research, development, and manufacturing of biopharmaceutical products. On January 5, 2016, the FBI arrested Li and seized his computer on which they found a number of GSK documents containing trade secret and confidential information which he had received from Xue. Xue previously pleaded guilty on August 31, 2018.

(3) Large-Scale Commercial Counterfeiting and Online Piracy

The Department continues to pursue significant, large-scale piracy and counterfeiting operations. In FY 2018, the Department has had a number of significant prosecutions, including those set forth below:

- *Orlando Pair Sentenced For Copyright Infringement Of Microsoft Products And Conspiracy To Commit Wire Fraud.* On December 1, 2017, Robert F. Stout, and Kasey N. Riley, a/k/a Kasey Stout, were sentenced to 18 months' imprisonment and 12 months of home detention, respectively, for conspiracy to commit wire fraud and copyright infringement relating to the sale of illegal activation keys for Microsoft products. As a part of their sentences, the Court also ordered them to pay $1,480,227, the proceeds of the charged criminal conduct.

- *Sacramento Man Sentenced To Prison For Criminal Trademark Infringement.* On December 15, 2017, Xavier L. Johnson was sentenced to two years and six months in

prison and three years of supervised release for trafficking in goods bearing counterfeit trademarks. From 2008 to 2011, Johnson and co-defendant Kristin Caldwell imported DVDs from China that contained counterfeit versions of children's movies.

- *Staten Island Man Sentenced For Trafficking Over $2.5 Million In Counterfeit Footwear Through Port Of Newark.* On January 23, 2018, Shi Wei Zheng was sentenced to 30 months in prison and two years of supervised release for attempting to distribute more than $2.5 million of counterfeit UGG-brand boots that were shipped into the Port of Newark. From September 2016 through February 2017, Zheng received certain shipping container numbers from an individual overseas that identified at least three containers containing counterfeit UGG boots. Cheng asked individuals working at the Port of Newark to remove the containers from the port before they could be examined by U.S. Customs and Border Protection. Once the containers were removed, Zheng directed that they be delivered to other individuals working for him, who would then distribute the boots in New Jersey and elsewhere.

- *Chinese National Pleads Guilty to Conspiracy and Trafficking of Counterfeit Apple Goods into The United States.* On February 2, 2018, Jianhua "Jeff" Li pleaded guilty for his role as a counterfeit distributor in a scheme to traffic and smuggle counterfeit electronics purporting to be Apple iPhones and iPads, from China into the United States. From July 2009 through February 2014, Li, working through his company, Dream Digitals, conspired with Andreina Becerra, Roberto Volpe, Rosario LaMarca, and others to smuggle and traffic into the United States from China more than 40,000 electronic devices and accessories, including iPads and iPhones, along with labels and packaging bearing counterfeit Apple trademarks. Li also received payments totaling over $1.1 million in sales proceeds from U.S. accounts into his bank accounts. Becerra, Volpe, and LaMarca have also pleaded guilty to their roles in the conspiracy. LaMarca was sentenced on July 20, 2017, to 37 months in prison. Volpe and Becerra were sentenced on October 15, 2018. Volpe was sentenced to 22 months in prison, and Beccerra was sentenced to three years of probation.

- *Owner of Sharebeast.com Sentenced for Copyright Infringement.* On March 22, 2018, Artur Sargsyan, of Glendale, California, was sentenced to five years in prison followed by three years of supervised release for his role in operating a massive file-sharing infrastructure that distributed approximately 1 billion copies of copyrighted musical works through Internet downloads. He was also ordered to pay restitution in the amount of $458,200 and to forfeit $184,768.87. Sargsyan owned and operated a number of websites including Sharebeast.com, Newjams.net, and Albumjams.com. Sargsyan pleaded guilty to copyright infringement on September 1, 2017.

- *New York Woman Sentenced for Trafficking Over $3 Million In Counterfeit Footwear And Handbags Through Port Of Newark.* On May 23, 2018, Xiao Xia Zhao pleaded guilty to trafficking in counterfeit goods. F In total, Zhao trafficked in thousands of pairs of fake Nike footwear, Louis Vuitton handbags, and other counterfeit items, with a total estimated retail value of over $3 million. From November 2013 through February 2017, Zhao received certain shipping container numbers from an individual overseas that

identified at least three containers containing counterfeit merchandise. Zhao asked individuals working at the Port of Newark to remove the containers from the port before they could be examined by U.S. Customs and Border Protection. On October 22, 2018, Zhao was sentenced to 18 months imprisonment and three years of supervised release.

- *California Sentenced for Copyright Infringement.* On July 23, 2018, Craig M. Vincent pleaded guilty to one count of criminal infringement of a copyright. Vincent admitted he used eBay to resell aviation navigational database updates in violation of Jeppesen Company's licensing agreement for a trademarked product called NavData. Jeppesen's NavData includes airport information, runway characteristics, waypoints, arrival routes, departure routes, terminal procedures and general information that a Global Positioning System or flight management computer needs to navigate an airplane to final destination. Doing business as Merlin Enterprises, Vincent sold NavData cards and required customers to return old data cards to him. On October 15, 2018, Vincent was sentenced to serve three years on federal probation.

- *Five Defendants Charged In Manhattan Federal Court With Multimillion-Dollar Counterfeiting Scheme.* On August 7, 2018, defendants Miyuki Suen, Jian Min Huang, Kin Lui Chen, Songhua Qu, and Fangrang Qu were arrested on charges of importing hundreds of thousands of athletic shoes from China into the United States. The defendants are each charged with one count of conspiring to traffic in counterfeit goods, and one count of trafficking in counterfeit goods. From at least in or about January 2016 up to and including in or about July 2018, the defendants imported at least 42 shipping containers holding an estimated more than 380,000 pairs of sneakers from China. Once these shoes arrived, the defendants added trademarked logos to the shoes, rendering them counterfeit. The estimated loss attributable to the defendants' efforts amounts to more than $70 million.

- *California Man Sentenced for Trafficking in Counterfeit Sports Apparel.* On August 10, 2018, Seyyed Ali Noori was sentenced to 12 months imprisonment and 12 months of supervised release for trafficking in counterfeit sports apparel, and ordered to pay restitution to victim companies, totaling $27, 565.51. Noori had pleaded guilty on March 30, 2018. Noori owned and operated Goldstar Wholesale LLC, a regional wholesale distributor based in Tracy, California, and also sold goods at the Galt Flea Market in Galt, California.

- *22 Charged With Smuggling Millions of Dollars of Counterfeit Luxury Goods From China Into the United States.* On August 16, 2018, six indictments and one criminal complaint were unsealed in federal court, charging a total of 22 defendants with illegally bringing into the United States millions of dollars of Chinese-manufactured goods by smuggling them through ports of entry on the East and West Coasts. Twenty-one defendants were arrested on charges, including conspiracy to traffic, and trafficking, in counterfeit goods; conspiracy to smuggle, and smuggling, counterfeit goods into the United States; money laundering conspiracy; immigration fraud and unlawful procurement of naturalization. The defendants played various roles in the trafficking of counterfeit goods manufactured in China, brought by ocean-going ships to the United

States in 40-foot shipping containers, smuggled through ports of entry disguised as legitimate imports and distributed throughout the country. The counterfeit goods included items such as fake Louis Vuitton and Tory Burch handbags, Michael Kors wallets, Hermes belts and Chanel perfume.

Domestic Training

During the past fiscal year, the Department provided a number of training programs for federal, state, and local prosecutors and agents investigating IP crimes. These training courses covered a range of IP enforcement issues and were designed to increase coordination between prosecutors and investigators as well as coordination among federal, state, and local law enforcement agencies. Examples of such training included:

- In October 2017, CCIPS, in conjunction with the Executive Office of U.S. Attorneys ("EOUSA"), presented a one-hour webinar for federal prosecutors on the prosecution of cases involving counterfeit microelectronics. The presentation included a background on microelectronics production and procurement, relevant law and policy, practical guidance in counterfeit trademark investigations, and included a case study.

- In October 2017, NSD, with support from CCIPS, organized and led the annual NSCS Training in McLean, Virginia. The NSCS training builds on the technical skills covered by the annual CHIP conference to address the added complexity of working with classified information and issues related to the investigation, prosecution, and disruption of crimes impacting national security.

- In January 2018, CCIPS was scheduled to present its Intellectual Property Crimes Seminar at the NAC. Citing the lapse in appropriations, DOJ's Office of Legal Education cancelled the seminar. The Seminar is an in-depth course on investigating and prosecuting trafficking of counterfeit goods and services, criminal copyright infringement, and theft of trade secrets, along with significant instruction on electronic evidence gathering for IP cases.

- In March 2018, CCIPS and the District of Kansas U.S. Attorney's Office presented on the trial and conviction of Weiqiang Zhang at the National Security Seminar on Export Control, Counterproliferation and Counterintelligence. Zhang, a former rice breeder at Ventria Biosciences in Kansas, provided proprietary rice seeds to members of a visiting Chinese delegation during their visit to the U.S. in 2013. Zhang was convicted in the District of Kansas of conspiracy to commit theft of trade secrets and related charges in February 2017.

- In April 2018, CCIPS presented at FBI Headquarters for approximately 25 FBI Supervisory Special Agents and Analysts on *United States v. Sinovel*. The presentation focused on tips for "investigating a case for trial."

- In April, June, and August 2018, CCIPS presented at Intellectual Property and Trade Enforcement Investigations course at the IPR Center Arlington, Virginia, to approximately 30 HSI and CBP agents. The presentation covered relevant law and policy, provide practical guidance in counterfeit trademark investigations, and include a case study.

- In June 2018, CCIPS hosted its annual CHIP Conference and Training at the NAC. Approximately 150 prosecutors attended the four-day event, which featured training on a wide range of investigative, litigation, legislative, and technology issues. The conference also included multiple breakout sessions, and an optional day with two tracks—a refresher track, and an advanced technology track.

- In July 2018, CCIPS presented to Naval Criminal Investigative Service (NCIS) and other federal agents at a day-long training in San Diego, California. The training, organized by the IPR Center, focused on Operation Chain Reaction, which targets counterfeit microelectronics in the government and military supply chains. The presentation covered relevant law and policy, practical guidance in counterfeit trademark investigations, and included a case study.

- In August 2018, CCIPS presented at FBI's 2018 National Intellectual Property Rights Training at the FBI Field Office in Dallas, Texas. The presentation was titled "What You Need for a Successful Trade Secret Theft Prosecution." CCIPS also presented a case study about the Sinovel prosecution. More than 50 FBI agents and other members of federal law enforcement attended. .

- In September 2018, CCIPS spoke at a symposium at FBI headquarters on the diversification of transnational crime in the Western Hemisphere. CCIPS gave a presentation focusing on the links between organized crime and intellectual property crime and cybercrime in Latin America as well as recent developments and trends in the region in these areas. The audience included approximately 150 people, primarily federal law enforcement agents and analysts.

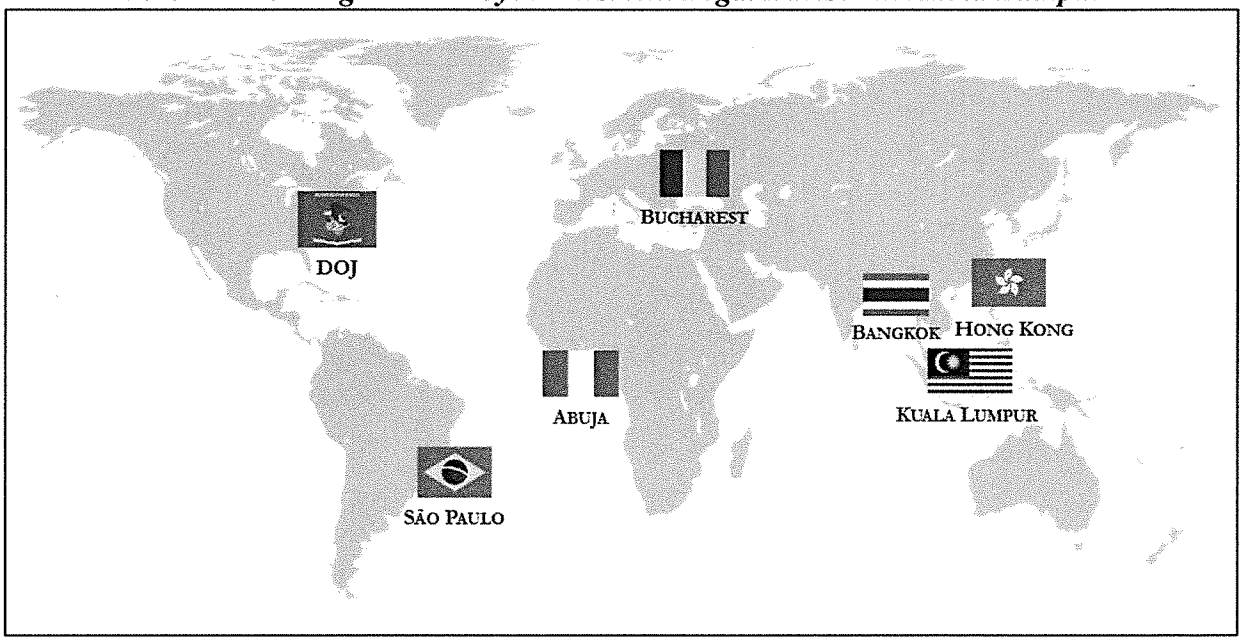
International Outreach and Training

Global IP crime, from the manufacture and worldwide distribution of counterfeit goods, to the sprawling online businesses designed to reap profits from the distribution of copyrighted works, continues to grow and change in an effort to stay ahead of law enforcement. As a world leader in efforts to combat criminal IP infringement, the Department actively seeks to develop training and technical assistance programs to assist other countries in effectively enforcing IP laws and reducing the trafficking of counterfeit and pirated goods. Despite budgetary constraints, in FY 2018, the Department worked extensively with its law enforcement counterparts around the world. The Department sought to engage foreign law enforcement through meetings of officials, ranging from the Attorney General to line attorneys and agents.

CCIPS and DOJ's Office of Overseas Prosecutorial Development, Assistance and Training ("OPDAT") worked with State Department grants and in cooperation with other United States agencies in FY 2018 to provide training to foreign officials on effective enforcement of IP laws. CCIPS's IP trainings are designed to increase cooperation between various law enforcement agencies with responsibility for IP offenses; to utilize various types of charges, including economic and organized crime statutes to combat IP crime; and to increase awareness amongst enforcement officials and the judiciary of the importance of reducing counterfeiting and piracy.

In FY 2018, the Department, with the assistance from the State Department, continued to expand the IPLEC program. Experienced DOJ attorneys now serve as regional IPLECs in Bangkok, Thailand; Bucharest, Romania; Hong Kong; Sao Paolo, Brazil; and Abuja, Nigeria.[8]

DOJ's IPLEC Program and Cyber Resident Legal Advisor in Kuala Lumpur



In addition to the Department's regional efforts through its IPLEC program, examples of DOJ's international engagement regarding various IP enforcement include:

ASIA

Presentation to Chinese Copyright Delegation. In November 2017, CCIPS presented on U.S. criminal copyright law, combatting online piracy, and international cooperation to a 17-person delegation from China's National Copyright Administration, Public Security Bureaus, and Cultural Market Enforcement Agency. The U.S. Patent and Trademark Office and OPDAT facilitated the meeting held in Washington, D.C.

Presentation to Pakistani Delegation: In November 2017, CCIPS presented to a delegation of Pakistani IP government officials and private IP attorneys. The discussion focused on U.S. intellectual property enforcement efforts and case studies. CCIPS also discussed Pakistani IP statutes and ways to bring them in-line with international best practices and norms through a comparative analysis with U.S. laws.

U.S.-China Joint Dialogue on Counterfeit Pharmaceuticals. In January 2018, CCIPS and DOJ Civil Division's Consumer Protection Branch, along with the Hong Kong IPLEC, met with six senior Chinese law enforcement officials from the Ministry of Public Security's Public Order Administration to discuss combatting the trafficking of counterfeit pharmaceuticals. The

[8] For more information about CCIPS's international outreach, see https://www.justice.gov/criminal-ccips/overseas-work.

delegation's trip was coordinated by CCIPS and the IPLEC through the U.S.-China Joint Liaison Group's ("JLG") Intellectual Property Criminal Enforcement Working Group. The JLG is designed to strengthen law enforcement cooperation between the United States and China across a range of issues, including intellectual property. Representatives from the FDA's Office of Criminal Investigations, National IPR Center, and the U.S. Patent and Trademark Office also met with the delegation.

USPTO Workshop on Proliferation of Counterfeit Products in India. In February 2018, the Hong Kong IPLEC traveled to New Delhi, India to serve as an instructor at a workshop organized by the USPTO's South Asia Office, with assistance from FDA-OCI, on "Combating the Proliferation of Substandard, Unregistered, Unlicensed and Falsified Health and Safety Regulated Products," with particular emphasis on counterfeit pharmaceuticals. Workshop participants included 59 Indian delegates, most from the Central Drugs Standard Control Organization (CDSCO); two delegates each from Nepal and Sri Lanka; as well as representatives from INTERPOL, Her Majesty's Revenue and Customs Service and the recently established Border Force of the United Kingdom, U.S. CBP, and the United Nations Universal Postal Union (UPU).

Training Events Promoting Intellectual Property Right Enforcement in Vietnam. In March 2018, the Hong Kong IPLEC and Bangkok IPLEC participated in a series of events promoting IPR enforcement in Vietnam. The Asia IPLECs co-sponsored with the U.S. Embassy and Vietnam's Ministry of Science and Technology (MOST) a roundtable on IP enforcement in a digital world. The IPLECs met with senior officials at the MOST Inspectorate, which is responsible for coordinating training events for all nine Government of Vietnam (GOV) agencies involved in IPR enforcement. The IPLECs also participated in a roundtable for GOV agencies involved in IPR criminal enforcement, including the Supreme People's Court, the Supreme People's Procuracy, and the Ministry of Public Security, as well as private attorneys representing IP rights holders. The IPLECs also gave an address on IP enforcement at Hanoi Law University, and the Hong Kong IPLEC participated in an American Chamber of Commerce (AmCham) roundtable on innovation and IP sponsored by AmCham as well as met with officials of the provincial Department of Science and Technology to discuss training needs.

Meeting with Chinese Media Group on Enforcement of Copyright Laws. In April 2018, CCIPS met with representatives from the Shenzhen Media Group (a state-owned media company that owns TV channels and radio stations) to discuss copyright enforcement issues as well as U.S. copyright law. Officials from the U.S. Patent and Trademark Office, U.S. Copyright Office, U.S. Trade Representative, and IPR Center also participated in the meeting.

Presentation at Trade Secrets Workshop in Taiwan. In April 2018, CCIPS, the Southeast Asia Resident Legal Advisor for Cybercrime, and the Hong Kong IPLEC, in conjunction with the FBI and the USPTO, presented a Trade Secrets Workshop in Taipei, Taiwan. The audience included approximately 175 Taiwanese prosecutors, judges and investigators, and covered Taiwan's Trade Secrets Act, including presentations and panels regarding identifying and articulating trade secrets, using protective orders, assessing loss in theft of trade secrets cases, and more.

Digital Video Conference with Taiwan on Intellectual Property Issues. In May and August 2018, CCIPS participated in a half-day interagency digital video conferences on IP issues in Washington, D.C., with 20 Taiwanese government officials including prosecutors from the Taiwanese Ministry of Justice. Specific topics included internet piracy, illicit streaming devices, textbook piracy, and amendments to the Taiwan Copyright Act.

Meeting with Chinese Law Enforcement Officials to Discuss Coordinated Intellectual Property Cases. In May 2018, CCIPS, and representatives from the National IPR Center, met with Chinese law enforcement officials to discuss ongoing case cooperation. This meeting is a continuation of CCIPS's work under the former U.S.-China Joint Liaison Group's ("JLG") Intellectual Property Criminal Enforcement Working Group ("IPCEWG"). The JLG was designed to strengthen law enforcement cooperation between the United States and China across a range of issues, including intellectual property, and was subsumed last fall into the U.S.-China Law Enforcement and Cybersecurity Dialogue. A CCIPS attorney, who served as co-chair of the IPCEWG, led the meeting. The Chinese delegation was led by a Deputy Director General of China's Ministry of Public Security, Economic Crime Investigation Department.

Presentation to Chinese Delegation on Intellectual Property Rights. In May 2018, CCIPS addressed a Chinese government delegation in Washington, D.C., on U.S. criminal enforcement of IP rights. The presentation was a part of the U.S. State Department's International Visitor Leadership Program.

Meeting with Korean Law Enforcement Officials on Combatting Counterfeit Pharmaceuticals. In May 2018, CCIPS met with officials from Korea's Ministry of Justice and Ministry of Food & Drug Safety to discuss best practices in investigating and prosecuting counterfeit pharmaceutical cases, as well as the take-down/seizures of related websites.

Forum on Criminal Intellectual Property Cases. In July 2018, the Hong Kong IPLEC participated in the Quality Brands Protection Committee (QBPC) 2018 Criminal IP Forum. The Hong Kong IPLEC served as a panelist discussing the potential for plea bargaining in criminal cases in China.

IPR Training for Vietnamese Judicial Officials. In July 2018, the Hong Kong IPLEC and CCIPS, along with HSI, met with justices of the Supreme People's Court of Vietnam and other Vietnamese judicial officials in Hanoi and Ho Chi Minh City, Vietnam to provide training on best practices and techniques for criminal enforcement of intellectual property rights. Over the past several years, Vietnam's national legislature has enacted significant amendments to strengthen the country's criminal intellectual property laws, but these changes have thus far not resulted in substantial improvements in enforcement. The program, organized by the Hong Kong, is designed to assist Vietnam's Supreme People's Court in developing guidance for lower courts to implement these new changes to Vietnam's criminal laws, and to improve enforcement of IP rights in Vietnam.

Colloquium on Intellectual Property Rights in Myanmar. In July 2018, the Bangkok IPLEC presented on criminal enforcement of intellectual property rights to an audience of judges from Myanmar at a USPTO/USAID-sponsored judicial colloquium on intellectual property rights.

Presentation to Thai Prosecutors on Intellectual Property Crime. In August 2018, the Bangkok IPLEC presented on criminal enforcement of IP cases to an audience of Thai public provincial public prosecutors at a USPTO-Thai Attorney General's Office-sponsored workshop. This was one of a series of such workshops throughout Thailand to roll out a new manual on criminally prosecuting IP violations developed with USPTO support by the Office of the Attorney General of Thailand for use by Thai public prosecutors.

Regional Workshop on Counterfeit Goods in Thailand. In August 2018, the Hong Kong and Bangkok IPLECs, along with the USPTO, presented the "Asia Regional Workshop on Criminal Enforcement Against Online Trade in Pirated Content and Counterfeit Goods." Approximately 120 police, prosecutors, and IP administrative officials from 15 Asian nations attended the workshop. HSI, FDA-OCI, the ASEAN Secretariat, and the EUIPO IP Key program also supported the workshop. Subsequently, on August 24, also in Bangkok, the Hong Kong and Bangkok IPLECs participated in opening the third meeting of the ANIEE, which was established in November 2016 as a successor to the ASEAN Working Group on IP Crime.

Presentation at Sixth Asian IP Crimes Enforcement Network Meeting. In September 2018, DOJ IPLECs in Hong Kong and Bangkok and CCIPS hosted the sixth meeting of the Asian IP Crimes Enforcement Network in Hong Kong. About ten countries from the region gathered to discuss methods to facilitate the exchange of successful investigation and prosecution strategies in combating domestic piracy and counterfeiting crimes, and how to strengthen communication channels to promote coordinated, multinational prosecutions of the most serious offenders. The meeting included panel discussions by law enforcement officials, presentations by representatives of affected industries, and technical and legal discussions from U.S. experts.

NORTH AFRICA AND THE MIDDLE EAST

Workshop on Intellectual Property Offenses Related to Commerce and Terrorism. In March 2018, the Nigeria IPLEC traveled to Kuwait, City, Kuwait to instruct on IP offenses in a workshop co-sponsored by the Kuwait Ministry of Commerce and Industry, Anti-Money Laundering and Counter-Terrorism Funding Administration (KMCI-AML/CFT) and DOJ OPDAT. The workshop was entitled "Investigating Fraudulent Business Transactions to Prevent Money Laundering and Terrorism Funding," and it included, in addition to the segments on IP offenses, sections on basic fraud investigations, indicators of fraud, interview techniques and strategies, evidence needed for prosecutions, and case scenarios.

Judicial Training Conference in Uzbekistan for Uzbekistani Judges. In June 2018, CCIPS participated in a three-day training conference in Tashkent, Uzbekistan for Uzbekistani judges focusing on protection of intellectual property rights. The U.S. Patent and Trademark Office, in conjunction with the U.S. Embassy in Tashkent, DOJ, and the Uzbekistani judiciary, organized the conference, which included around 20 participants. CCIPS gave five presentations on various topics involving intellectual property and IPR enforcement in the U.S. and Uzbekistan. CCIPS also led a discussion of a case study and participated in additional panels and discussions as well as a reception at a local nongovernmental organization for a mock trial program they organized in Chorvoq, Uzbekistan for Uzbekistani and Afghan law enforcement.

Presentation to Middle Eastern and Northern African Judges at USPTO's Intellectual Property Judicial Exchange. In August 2018, CCIPS presented at the U.S. Patent and Trademark Office's Middle Eastern and Northern Africa Intellectual Property Judicial Exchange. The audience consisted of forty judges from Algeria, Egypt, Jordan, Kuwait, Oman, the Kingdom of Saudi Arabia, and United Arab Emirates. The four-day program was designed to provide a comprehensive overview of U.S. intellectual property law. CCIPS presented on DOJ's priorities in combatting intellectual property infringement and provided an overview of criminal trademark, copyright, and theft of trade secrets law as well as sentencing issues.

CENTRAL AND SOUTH AMERICA

Regional Intellectual Property Rights Enforcement Program in Brazil. In March 2018, the Brazil IPLEC participated in a regional IPR enforcement program organized by HSI Colombia and the IPR Center for approximately 40 police, prosecutors, and customs officials from the Ecuador, Colombia, Peru, and Guatemala. The IPLEC focused on IPR prosecutions involving the Internet, and provided an overview of online investigation principles and the basics of electronic evidence. The IPLEC also visited the Port in Cartagena, and met with both CBP and Colombian customs officials to discuss their challenges coping with the importation of counterfeit goods.

South America Regional Workshop on Measures Against Trade in Illicit and Counterfeit Agricultural Chemicals. In April 2018, CCIPS assisted DOJ IP Law Enforcement Coordinator Dan Ackerman, who is based in Sao Paulo, in hosting a DOJ and USPTO-sponsored "Workshop on Measures Against Trade in Illicit and Counterfeit Agricultural Chemicals" in Iguazu Falls, Brazil. Approximately 50 government officials from regulatory, customs, investigative, and prosecutorial agencies in the United States, Brazil, Paraguay and Argentina gathered to discuss methods to facilitate the exchange of successful enforcement strategies in combating trade in illicit and counterfeit pesticides. The program included panel discussions by law enforcement officials, presentations by industry representatives, and technical and legal discussions from U.S. experts. DOJ ENRD, EPA, CBP, HSI and USPTO representatives also served as instructors.

USPTO Judicial Workshop on the Protection and Enforcement of Intellectual Property Rights. In April 2018, CCIPS presented to a group of judges from Latin American countries, including Argentina, Brazil, Costa Rica, Dominican Republic, Panama, Peru, on the topic of U.S. Criminal Prosecution of Intellectual Property Crimes in the Digital Domain. Together, with Chief Judge Gustavo Gelpi of the U.S. District Court of Puerto, the group discussed a variety of topics, including the importance of international cooperation, public-private sector partnerships, and careful consideration of public health and safety issues. .

Participation in U.S.-Cuba Law Enforcement Dialogue (LED). In May 2018, in Washington, D.C., CCIPS participated in the U.S.-Cuba LED as a technical expert on cybercrime and intellectual property crime. The LED is a high-level dialogue designed to strengthen law enforcement cooperation between the United States and Cuba across a range of issues. Topics for discussion included legal cooperation, counterterrorism, human trafficking, human smuggling, counter-narcotics, anti-money laundering, and cyber issues. Representatives from the State

Department, DHS, ICE-HSI, U.S. Coast Guard, HHS, INTERPOL, DEA, and FBI also attended on behalf of the United States.

IPR Enforcement Program in Uruguay. In May 2018, the Brazil IPLEC participated in a regional IPR enforcement program in Montevideo, Uruguay, organized by HSI Argentina and the IPR Center for police, prosecutors, and customs officials from Uruguay and Paraguay. The IPLEC focused on IPR prosecutions involving the Internet, and provided an overview of online investigation principles, cyber-tracing techniques, and basics of electronic evidence. The IPLEC also spoke about international collaboration to obtain electronic evidence in criminal cases.

Training on Electronic Evidence in Copyright Infringement Cases. In July 2018, the Brazil IPLEC and USPTO trained approximately 60 Peruvian judges on best practices in handling of electronic evidence in digital copyright infringement cases. Two U.S. District Court judges as well as several US rights holders also served as instructors for the program. Participants learned about trending legal and policy issues in the acquisition and authentication of electronic evidence in digital copyright infringement cases as well as other cyber-enabled crime.

Training for Law Enforcement and Prosecutors on Intellectual Property Infringement. In July 2018, the Brazil IPLEC, CCIPS, and USPTO trained approximately 90 police and prosecutors from various Central American countries on best practices in IP infringement cases involving health and safety products in Santo Domingo, Dominican Republic. The program highlighted counterfeit pharmaceuticals and cosmetics case studies and addressed how authorities in different countries deal with the investigative and evidentiary issues that arise in these cases. Multiple pharmaceutical companies as well as Western Union presented on how they can assist law enforcement in these cases.

Training on Electronic Evidence in Intellectual Property Right Crime. In July 2018, the Brazil IPLEC and CCIPS trained approximately 60 Brazilian police and prosecutors from 16 Brazilian states and multiple cities within São Paulo state on the handling of electronic evidence in cybercrime investigations, including IPR crime. Facebook/Instagram and Microsoft participated in a panel for providers to share their insights on collaboration with law enforcement, especially on requests for overseas data. The program included a practical tabletop exercise on locating a target of a crime using open source applications, third-party data, and traditional methods of investigation.

Training on Intellectual Property Rights Cases in Mexico. In August 2018, the Brazil IPLEC and USPTO trained 30 Mexican prosecutors, police, and customs officials on best practices in IPR criminal investigations and prosecutions. The IPLEC co-presented on these issues along with the chief of the IP crimes section at the Mexican Attorney General's office (PGR).

Training with USPTO for Mexican Law Enforcement and Prosecutors. In August 2018, the Brazil IPLEC trained approximately 100 Mexican prosecutors, police, and customs officials on best practices in IPR criminal investigations and prosecutions at National IPR Center and Mexican Customs (SAT)-sponsored program held at the SAT headquarters in Mexico City. The IPLEC co-presented on these issues along with the USPTO Attaché for Mexico, Central America, and the Caribbean.

Training for Northern Triangle Prosecutors, Judges, and Law Enforcement on Intellectual Property Crime Prosecutions. In September 2018, CCIPS presented at a workshop on combatting intellectual property crime prosecutions at the International Law Enforcement Academy in San Salvador, El Salvador. The U.S. Patent and Trademark Office organized the workshop, and participants included judges, prosecutors, law enforcement, and customs officials from El Salvador, Honduras, and Guatemala. CCIPS presented on prosecuting intellectual property crime and sentencing issues, and also participated on panels addressing international cooperation, collaboration with customs officials, and the use of electronic evidence in intellectual property prosecutions.

Presentation at Workshop on Intellectual Property Rights. In September 2018, CCIPS presented at the Regional Workshop on Border Enforcement of Intellectual Property Rights in Chetumal, Mexico. Law enforcement, customs agents and prosecutors from Mexico, Guatemala, and Belize attended the workshop, organized by the U.S. Patent and Trademark Office. CCIPS presented on investigating and prosecuting intellectual property offenses, and participate on panels discussing infringement determinations and promoting regional cooperation.

EUROPE

EIPPN Third Annual Workshop. In October 2017, the Romania IPLEC provided an overview of the available legal assistance and cooperation channels with the U.S. in IP and cybercrime cases to approximately 70 specialized IP prosecutors from 28 countries at a two-day workshop in The Hague. The European Union Intellectual Property Office (EUIPO), Eurojust, and the European Intellectual Property Prosecutors Network (EIPPN) organized the program, which was the EIPPN's third annual workshop.

Open World Program on Criminal Enforcement of Intellectual Property Rights. In October 2017, CCIPS met with six Intellectual Property Rights specialists from Belarus, as part of the Open World Program at the Library of Congress. The Open World Leader Center, an independent government agency of the United States Congress, administers the program, which is designed to enhance understanding and cooperation between the Congress, American communities, and global leaders. Attendees were Belarusian nationals who work on intellectual property matters. The discussion focused on how U.S. law enforcement officials investigate, prosecute, and deter criminal intellectual property crimes.

Training Program Focused on Intellectual Property Violations and Computer Crime. In December 2017, in Bucharest, Romania, the Romania IPLEC and DOJ Intermittent Legal Advisor organized a two-day training program on combatting IP violations and investigating financial and computer crime for 30 judges, prosecutors, and law enforcement officers from Romania's Economic Crime, Organized Crime, and Anticorruption Divisions of the Prosecutor General's Office. FBI, DEA, NDIL AUSA, and a Council of Europe representative also participated in the program.

Presentation to American Chamber of Commerce in Romania. In February 2018, the Romania IPLEC presented to the American Chamber of Commerce (AmCham) in Romania about

improving cooperation and coordination in criminal IP cases and connecting resources and efforts of the private sector with law enforcement partners on national and international levels. The IPLEC provided an overview of DOJ's criminal IP enforcement efforts and the IPLEC program, including how the Romania IPLEC can work with rights holders in the region, other resources for assistance in IP matters, and best practices in working with law enforcement.

EUIPO and EIPPN Annual Conference. In April 2018, the Romania IPLEC participated in the European Union Intellectual Property Office (EUIPO) and the European Intellectual Property Prosecutors Network (EIPPN) annual conference in Alicante, Spain. Approximately 68 prosecutors, law enforcement officers, academia and private industry representatives from 26 countries attended. The program addressed health and safety aspects of intellectual property rights (IPR) violations, Internet protocol TV (IPTV) crime trends, and best practices for combating these crimes. The Romania IPLEC provided an overview of the United States' experience with IPR and health and safety, with special emphasis on counterfeit pharmaceuticals, personal care products, automotive parts, electronics and toys, and discussed recent developments in the legal assistance and cooperation channels available with the United States in IPR and cybercrime cases.

Meeting on Arbitration and Mediation of Intellectual Property Rights Cases. In April 2018, at the Romanian-American University in Bucharest, the Romania IPLEC and FSN participated in a meeting focused on mediation and arbitration in IPR cases organized by World Intellectual Property Organization (WIPO) in cooperation with the Romanian Copyright Office (ORDA) to mark the 2018 World IP Day. The IPLEC presented an overview of arbitration and mediation in IPR cases in the U.S., the IPLEC program, and avenues for assistance with the U.S. in IPR cases.

Training on Trade Secrets in Austria. In June 2018, the Romania IPLEC participated in two events hosted by the U.S. Embassy in Austria and the Federation of Austrian Industries. The events were designed to share international best practices and to help strengthen Austria's trade secrets legal regime. In the morning session, the Romania IPLEC participated in a trade secrets expert roundtable during which policymakers, officials, and business representatives from Europe and the United States exchanged best practices and discussed the development of effective trade secret laws. In the evening session, over 40 representatives from the Austrian business community attended the stakeholder event, and the Romania IPLEC participated in a panel session at that event designed to raise awareness about the importance of strong trade secrets protection.

National Conference at the Studies Institute for Public Order. In July 2018, the Romania IPLEC, in partnership with the Romanian counterparts, organized two joint workshops for Romanian investigators and prosecutors. 46 police investigators focusing on IP enforcement attended the first day-and-a-half workshop as part of their three-day annual national conference at Studies Institute for Public Order (ISOP). Subsequently, twenty-five prosecutors at the National Institute for Magistracy (INM) attended the second day-and-a-half workshop.

Workshop with USPTO Regarding Intellectual Property Rights Protection in Greece. In July 2018, the Romania IPLEC, in partnership with the USPTO and HSI, organized a joint two-day

workshop for law enforcement and judicial officials as well as industry involved in IPR protection in Greece. Forty-eight investigators, prosecutors and judges attended the workshop.

Judicial Training Conference for Armenian Judges. In September 2018, CCIPS participated in a three-day training conference at the USPTO on the protection of intellectual property rights for Armenian judges handling criminal cases at the trial, appellate, or administrative level. The conference was organized by USPTO in conjunction with the U.S. Embassy in Yerevan, DOJ, and the Armenian judiciary, and included around 20 participants. Armenia has one of the highest rates of piracy and counterfeiting in the world. CCIPS presented on relating to IPR enforcement in the U.S. and Armenia, and also participated in additional panels and discussions.

SUB-SAHARAN AFRICA

IP Meeting with Nigerian Officials. In February 2018, the Nigeria IPLEC traveled to Lagos to hold a series of meetings with IP stakeholders. Meeting attendees included representatives from the Nigerian American Chamber of Commerce (AmCham), National Agency for Food and Drug Administration and Control, Nigerian Copyright Commission, and International Trademarks Association.

Intellectual Property Workshop in Zimbabwe. In July 2018, the Nigeria IPLEC participated in WIPO and ARIPO's Training of Trainers IP Workshop. Representatives from thirteen of the nineteen member countries attended. The Nigeria IPLEC presented on U.S. perspectives on IP in Africa and on the elements of trademark counterfeiting. This was the first time WIPO and ARIPO have partnered with DOJ in the region, and the Nigeria IPLEC looks forward to further collaboration with these organizations.

Western Africa Workshop on Law Enforcement Capacity and Regional Coordination in Combatting Pharmaceutical Crimes. In August 2018, the Nigeria IPLEC led the Western Africa Workshop to Build Enforcement Capacity and Improve Regional Coordination in Combatting Pharmaceutical Crimes at the West Africa Regional Training Center in Accra, Ghana. Police, prosecutors, health regulatory officials, gendarmerie, investigative magistrates and customs officials participated from Nigeria, Ghana, Benin, Togo, Burkina Faso, Cameroon, and Niger. In addition to the Nigeria IPLEC, U.S. law enforcement and prosecutors as well as a Nigerian prosecutor, an INTERPOL official, and industry representatives served as workshop facilitators and instructors.

Dialogue on Anti-Piracy and Law Enforcement Issues. In August 2018, the Nigeria IPLEC convened numerous stakeholders in Nigeria's creative industry for a strategic dialogue on anti-piracy and enforcement issues at the American Guest Quarters at the U.S. Consulate in Lagos, Nigeria. In the morning session, the IPLEC team met with individuals from the literary and software sector, and in the afternoon session, they met with individuals representing the entertainment/art sector.

Outreach to the Private Sector

The Department continues to reach out to the victims of IP crimes in a wide variety of ways, including during the operational stages of cases and through more formal training programs and conferences. For example, in FY2018, CCIPS organized and planned its Eleventh Annual IP Industry and Law Enforcement Meeting held in Washington, D.C, in October 2017. The yearly meeting provides representatives from a broad range of industries with an opportunity to communicate directly with the law enforcement agents and prosecutors most responsible for federal criminal enforcement of IP law at the national level. This year, Deputy Attorney General Rod Rosenstein provided keynote remarks, and several senior DOJ and law enforcement officials, including Acting Assistant Attorney General Kenneth Blanco and officials from FBI, ICE-HSI, CBP, and FDA participated in the meeting. Approximately 90 government and industry representatives attended the meeting, including senior representatives from a broad range of industries such as pharmaceuticals, software, luxury goods, electronics, apparel, motion pictures, music, consumer goods, and automobiles.

In the past year, the Criminal Division's high-level officials and CCIPS attorneys, as well as the Civil Division's Consumer Protection Branch attorneys, have also presented at a variety of domestic and international conferences, symposia, workshops, and events attended by IP rights holders and law enforcement officials. These events included, among others:

- In October 2017, CCIPS presented at Michigan State University's Center for Anti-Counterfeiting and Product Protection (A-CAPP) Brand Protection Strategy Summit on a panel entitled "Organizational Adaptation and the Changing Nature of E-Commerce Retailers." The discussion focused on the changes to intellectual property rights enforcement in an age of increased e-commerce transactions, and addressed certain key factors affecting the evolving e-commerce landscape, including the multifaceted role of consumers, the nature and scope of collaborations between brand owners and e-commerce sites, and the impact of globalization on counterfeiters and their organizations.

- In November 2017, CCIPS addressed approximately 100 members of the International Trademark Association (INTA) Anticounterfeiting Committee as part of INTA's annual meeting in Washington, D.C. CCIPS discussed the roles of the section and other DOJ components, the CHIP Network, and the IP Law Enforcement Coordinator program in combatting intellectual property crime, with a particular focus on trademark counterfeiting and the international trafficking of fake hard goods.

- In November 2017, CCIPS participated in a panel discussion to an audience of approximately 100 intellectual property industry representatives and law enforcement officials at the 2017 IPR Center Symposium. The symposium was entitled "Solving the E-Commerce Puzzle," and included panels on topics such as fraud protection for consumers and business, efforts to reduce sale of counterfeits in online marketplaces such as eBay, Amazon and Alibaba, and challenges facing law enforcement.

- In March 2018, CCIPS attended meetings with the Automotive Anti-Counterfeiting Council (A2C2) and U.S. government representatives. The Intellectual Property

Enforcement Coordinator (IPEC) organized the roundtable discussion focused on A2C2's current and future initiatives as well as opportunities for further collaboration with the IPEC and other U.S. government agencies. The IPR Center hosted an additional meeting that consisted briefings and discussions focused on the sales of airbags and other automotive parts on e-commerce platforms as well as sharing best practices by industry and future training opportunities for law enforcement.

- In March 2018, CCIPS and NSD CES presented to the Electronic Components Industry Association (ECIA) Board in Crystal City, Virginia, and provided an overview of DOJ's criminal IP and export control enforcement efforts as well as best practices in identifying and reporting criminal activity. Approximately 20 executives from major electronic component manufacturers and their authorized distributors attended.

- In April 2018, CCIPS presented for the New York and New Jersey Intellectual Property Law Associations at a half-day conference entitled, "Trade Secrets / Cybersecurity: Protecting Your Corporate Client's Information." CCIPS's presentation, entitled "Cybercrime and Intellectual Property Crime: A Team Effort," focused on the importance of developing relationships with law enforcement in advance of an incident, and reaching out to law enforcement as soon as an incident does occur. More than 100 attorneys attended the presentation.

- In April 2018, CCIPS presented at the American Bar Association Intellectual Property Section's 33rd Annual Spring Conference in Arlington, Virginia. CCIPS was part of a panel on "The Dark Side of Knock-Off's." CCIPS's presentation focused on the challenges of investigating and prosecuting counterfeiting and how victims can work more effectively with law enforcement to deter counterfeiting. Approximately 100-150 IP attorneys attended the presentation.

- In April 2018, the Civil Division's Consumer Protection Branch presented to the Pharmaceutical Security Institute's 33rd General Assembly in McLean, Virginia, on prosecuting counterfeit drug cases. The presentation focused on federal prosecution priorities and recent cases involving counterfeit drugs.

- In May 2018, CCIPS and the IPR Center co-hosted a half-day meeting of the Counterfeit Microelectronics Working Group, which meets at least twice a year to discuss ways to detect and prevent counterfeit microelectronics in the U.S. supply chain. CCIPS, in conjunction with the IPR Center and industry partners, organized the meeting. Over 60 industry, government, and law enforcement representatives attended the meeting.

- In May 2018, CCIPS participated in a panel discussion at the International AntiCounterfeiting Coalition's (IACC's) Spring Conference in Seattle, Washington. CCIPS, and co-panelists from HSI, FBI, City of London Police, and the USPTO, addressed "Government Perspectives on Trends in and Evolution of Anti-Counterfeiting Enforcement." Topics included innovative enforcement programs at the national level and international, intergovernmental cooperation.

- In June 2018, the Civil Division's Consumer Protection Branch moderated a panel at the Partnership for Safe Medicine's Interchange in Washington, D.C. The meeting brought together policymakers, families of counterfeit drug victims, law enforcement, healthcare professionals, patient advocates, and pharmaceutical manufacturers and focused on the dangers of counterfeit drugs, particularly the upsurge in counterfeit opioids.

- In July 2018, CCIPS presented at the Smithsonian Museum of American History as part of the National Trademark Exposition. CCIPS served on a panel entitled, "Counterfeits and Con Artists: The Real Dangers and Costs of Fake Goods." The president of the International Trademark Association and a USPTO Enforcement Team representative also participated on the panel.

- In August 2018, CCIPS presented for a live-stream hosted by the IP Owners Association. The presentation was entitled, "IP Crime and Cybercrime: A Team Effort" and focused on the importance of developing relationships with law enforcement in advance of an IP or cyber incident, and communicating with law enforcement as soon as an incident does occur. The presentation was live-streamed to over 100 participants.

- In August 2018, CCIPS and the Civil Division Consumer Protection Branch participated in a Roundtable on Counterfeit Drugs at USPTO. Participants included public health researchers, economists, and U.S. Government representatives. The roundtable focused in particular on the problem of internet sales of counterfeit drugs directly to consumers.

- In September 2018, CCIPS presented to the International Trademark Association as part of its program on U.S. Federal Government's Work on IP Enforcement, Outreach, and Education. The presentation addressed the Department of Justice's work investigating, prosecuting, and deterring intellectual property crime and how the private sector can partner with law enforcement to address these serious crimes.

- In September 2018, CCIPS and the Civil Division's Appellate Section took part in a panel discussion in Los Angeles addressing the U.S. government role in copyright enforcement for an audience of approximately 400 representatives of the entertainment and copyright content industries.

- Throughout FY2018, DOJ CHIP AUSAs presented at China IP Road Shows, sponsored by the USPTO in Denver, Colorado; Salt Lake City, Utah; Indianapolis, Indiana; Chicago, Illinois; Portland, Oregon; Seattle, Washington; San Jose and San Francisco, California; Nashville, Tennessee; Louisville, Kentucky; Iowa City, Iowa; Kansas City, Missouri; and New York City. With the China IP Road Shows, the USPTO is partnering with a variety of organizations across the country — including universities, USPTO regional offices, business groups, state and local governments, and other federal agencies — to present a series of one-day events that delve into the details of how to better protect IP in China. These one-day events bring to local businesses and stakeholders the expertise and knowledge of the USPTO's China specialists as well as that of special

invited guests, and have been tailored to address the needs of the specific locale in which it is held.

Several years ago, NSD placed additional focus on the protection of national assets from the threats of nation states, including economic espionage and trade secret theft. These changes included creating a new Deputy Assistant Attorney General position focusing on protecting national assets. Pursuant to this increased focus over the last several years, NSD leadership and other attorneys have reached out to senior managers and counsel at hundreds of companies over the last year to educate them about the Department's resources and efforts to combat economic espionage and trade secret theft and other national security threats. These outreach efforts have included presentations at universities and think tanks, cybersecurity summits and roundtable discussions, as well as one-on-one meetings with senior executives at Fortune 500 and other companies. The NSCS Network also periodically disseminated talking points and other resources to its members nationwide to facilitate their outreach to companies and other organizations in their home districts and facilitated FBI field offices' efforts to educate AUSAs on the national security threats in their districts and to include them in FBI's outreach efforts in their districts.

The Department maintains two websites that, among other things, provide the public with information on the Department's IP enforcement efforts, assist victims in understanding where and how to report an IP crime, and provide guidance on case referrals. Those sites can be found at https://www.justice.gov/iptf and https://www.cybercrime.gov. The National IPR Center also has a website where the public can report IP theft. That site can be found at https://www.iprcenter.gov.

(a)(7)(C) Investigative and Prosecution Activity of the Department with Respect to IP Crimes

In addition to the examples of successful prosecutions listed above, there are of course hundreds of other worthy cases that could be cited. As demonstrated by the cases highlighted above, the Department has sought to increase the quality and scope of its investigations and prosecutions over the past years. Numerical statistics do not adequately convey the quality or complexity of these prosecutions, but they provide some insight into the effectiveness and impact of the Department's prosecution efforts. Accordingly, we have provided the chart below that contains statistics for FY 2018, listing the number of defendants and cases charged, the number of defendants sentenced, and the length of those sentences.[9] Section 404(b) of the PRO IP Act

[9] Case statistics were compiled by the EOUSA. The chart includes data on criminal cases/defendants where the following charges were brought as any charge against a defendant: 17 U.S.C. § 506 (criminal copyright infringement); 17 U.S.C. §§ 1201 to 1205 (circumvention of copyright protection systems); 18 U.S.C. §§ 1831 (economic espionage) & 1832 (theft of trade secrets); 18 U.S.C. § 2318 (counterfeit labeling); 18 U.S.C. § 2319 (criminal copyright infringement); 18 U.S.C. § 2319A (live musical performance infringement); 18 U.S.C. § 2319B (unauthorized recording of motion pictures); 18 U.S.C. § 2320 (trafficking in counterfeit goods); and 47 U.S.C. §§ 553 & 605 (signal piracy). The statutes were grouped together to eliminate double-counting of cases and/or defendants where more than one statute

also requests statistics on the number of arrests made. Please see the Annual Report of the Federal Bureau of Investigation, provided pursuant to Section 404(c) of the PRO IP Act, for an accounting of arrest statistics.

District Totals	FY 2018
Investigative Matters Received by AUSAs	189
Defendants Charged	117
Cases Charged	67
Defendants Sentenced	65
No Prison Term	36
1-12 Months	12
13-24 Months	7
25-36 Months	4
37-60 Months	3
60 + Months	3

was charged against the same defendant. However, this chart may not include cases or defendants if only a conspiracy to violate one of these offenses was charged.

In addition, we have provided the chart below with FY 2018 statistics for criminal IP cases broken down by type of charge.[10]

Charge	Cases charged	Percentage
Trademark *Trafficking in counterfeit goods, 18 U.S.C. § 2320*	53	77.9%
Copyright *Criminal copyright infringement, 17 U.S.C. § 506; 18 U.S.C. § 2319* *Counterfeit labels, 18 U.S.C. § 2318* *DMCA, 17 U.S.C. § 1201*	4 0 0	5.9% 0% 0%
Economic Espionage Act *Economic espionage, 18 U.S.C. § 1831* *Theft of trade secrets, 18 U.S.C. § 1832*	1 10	1.5% 14.7%
Total	**68**	**100%**

(a)(7)(D) Department-Wide Assessment of the Resources Devoted to Enforcement of IP Crimes

The Criminal Division currently devotes fourteen full-time attorneys, along with paralegals and support staff, in CCIPS to IP issues. CCIPS also provides substantial support to the IPR Center, assigning at least one attorney, and sometimes more, to help identify and de-conflict investigative leads, as well as develop and execute national enforcement initiatives.

The CHIP Network consists of AUSAs who are specially trained in the investigation and prosecution of IP and computer crimes. Every U.S. Attorney's Office has at least one CHIP attorney, and those districts that have historically faced the highest concentration of IP and high-tech crimes tend to have multiple CHIP attorneys.

Over the last year, more than twenty NSD attorneys have worked on hacking investigations (most of which involve the theft of information, including but not limited to trade secrets) and economic espionage investigations. As described above, the NSCS Network consists of more than 100 AUSAs and attorneys at Department headquarters who receive specialized annual training in the investigation and prosecution of national security cyber offenses, including the theft of IP and other information.

Under the IPLEC program, DOJ has had a Department attorney stationed in Bangkok, Thailand, since January 2006 to handle IP issues in Asia. Between November 2007 and March

[10] EOUSA compiled the statistics for number of cases charged broken down by IP statute. These statistics may not reflect cases where only a conspiracy to violate one of these offenses was charged, and there may be double-counting of cases where more than one statute was charged in the same case.

2011, a separate DOJ attorney was stationed in Sofia, Bulgaria, in order to handle IP issues in Eastern Europe. While funding for this position expired in 2011, DOJ has worked with the Department of State to post a DOJ attorney in Bucharest, Romania since 2015 to continue to handle IP issues in that region. DOJ also expanded its IPLEC program in FY 2015 by placing a DOJ attorney in Brasilia, Brazil, for a six-month term. With the assistance of the State Department, DOJ expanded the IPLEC program in FY 2016 by posting new regional IPLECs in Hong Kong and Sao Paolo, Brazil. Most recently, in FY 2017, the State Department and DOJ prepared fielded a new IPLEC position in Abuja, Nigeria. The Nigeria IPLEC deployed in October 2017, bringing the total number of regional IPLECs up to five DOJ prosecutors.

In addition to evaluating digital evidence, the CCIPS Cybercrime Lab technicians have provided extensive training on the use of digital forensics tools in IP cases to law enforcement audiences around the world.

IP enforcement is also an integral part of the mission of four sections of the Department's Civil Division: the Intellectual Property Section, the National Courts Section, the Consumer Protection Branch, and the Civil Appellate Staff. Through the Civil Division's Intellectual Property Section, the Department brings affirmative cases when United States' IP is infringed, including Uniform Domain-Name Dispute-Resolution Policy proceedings where domain owners have used trademarks owned by the United States in a manner that is likely to confuse the public. The National Courts Section initiates civil actions to recover various penalties or customs duties arising from negligent or fraudulent import transactions, many of which include importation of counterfeit goods. The National Courts Section also defends CBP enforcement of the ITC's Section 337 exclusion orders at the Court of International Trade; these orders are an important tool for patent enforcement. The Consumer Protection Branch conducts civil and criminal litigation under the Food, Drug, and Cosmetic Act, including prosecuting counterfeit drug and medical device offenses and assisting AUSAs throughout the country with their counterfeit pharmaceutical and device cases. Finally, the Civil Appellate Staff represents the United States in copyright and trademark cases in the courts of appeals, including participating as an amicus in private IP litigation involving important government interests and defending decisions of the Copyright Office and the U.S. Patent and Trademark Office against constitutional and statutory challenges.

(a)(8) Efforts to Increase Efficiency

> *"(8) A summary of the efforts, activities, and resources that the Department of Justice has taken to—*
>
> *(A) minimize duplicating the efforts, materials, facilities, and procedures of any other Federal agency responsible for the enforcement, investigation, or prosecution of intellectual property crimes; and*
>
> *(B) enhance the efficiency and consistency with which Federal funds and resources are expended to enforce, investigate, or prosecute intellectual property crimes, including the extent to which the Department has utilized existing personnel, materials, technologies, and facilities."*

The Department works hard to ensure the effective use of limited resources devoted to fighting IP crime. One of the most important ways to reduce duplication of effort is to ensure that law enforcement agencies are pursuing unique case leads, and that prosecutors are not following prosecution strategies that duplicate those in other districts. To that end, CCIPS continues to provide ongoing support to the IPR Center in Arlington, Virginia. Among other things, the IPR Center serves as an investigation clearinghouse for FBI, ICE-HSI, CBP, FDA, and other agencies. CCIPS also works closely with the CHIP Network to assist in coordinating national prosecution initiatives. Along similar lines, NSD works closely with the NSCS Network to assist in coordinating national prosecution initiatives designed to counter the national security cyber threat. Department attorneys will continue to work with the IPR Center and NCIJTF to identify and de-conflict investigative leads, as well as assist the CHIP and NSCS Networks to ensure that investigations and prosecutions are streamlined, not duplicated, and that charges are brought in the appropriate venue.

Appendix A – Glossary

A2C2	Automotive Anti-Counterfeiting Council
AUSA	Assistant U.S. Attorney
BJA	Bureau of Justice Assistance
CBP	Customs and Border Protection
CCIPS	Computer Crime and Intellectual Property Section
CES	Counterintelligence and Export Control Section
CHIP	Computer Hacking and Intellectual Property
DMCA	*Digital Millennium Copyright Act*
DOJ	Department of Justice
EOUSA	Executive Office for United States Attorneys
FBI	Federal Bureau of Investigation
FBI's Annual Report	FBI Fiscal Year 2017 Report to Congress on Intellectual Property Enforcement
FY 2017	Fiscal Year 2017
IC	Integrated circuits
ICE-HSI	Immigration and Customs Enforcement's Homeland Security Investigations
IP	Intellectual property
IPCEWG	IP Criminal Enforcement Working Group
IPEC	Intellectual Property Enforcement Coordinator
IPEP	Intellectual Property Enforcement Program
IPLEC	Intellectual Property Law Enforcement Coordinator
IPR Center	National Intellectual Property Rights Coordination Center
JLG	U.S.-China Joint Liaison Group
NAC	National Advocacy Center
NCIJTF	National Cyber Investigative Joint Task Force
NSCS	National Security Cyber Specialists
NSD	National Security Division
NW3C	National White Collar Crime Center
OJP	Office of Justice Programs
OPDAT	Office of Overseas Prosecutorial Development, Assistance and Training

PRC	People's Republic of China
PRO IP Act	*Prioritizing Resources and Organization for Intellectual Property Act of 2008*
USPTO	U.S. Patent and Trademark Office

February 6, 2020

Twitter (https://twitter.com/intent/tweet?text=Confronting%20the%20China%20Threat&url=https://www.fbi.gov/news/stories/wray-addresses-china-threat-at-doj-conference-020620) Facebook (https://www.facebook.com/sharer/sharer.php?u=https://www.fbi.gov/news/stories/wray-addresses-china-threat-at-doj-conference-020620&t=Confronting%20the%20China%20Threat) Email (mailto:?Subject=%22Confronting%20the%20China%20Threat%22&body=https://www.fbi.gov/news/stories/wray-addresses-china-threat-at-doj-conference-020620)

Confronting the China Threat

Director Wray Says Whole-of-Society Response is Needed to Protect U.S. Economic and National Security

(https://www.fbi.gov/image-repository/wray-doj-china-initiative-conference-020620.jpg)

FBI Director Christopher Wray speaks at the Department of Justice China Initiative Conference held February 6, 2020 at the Center for Strategic and International Studies in Washington, D.C.

China is threatening the U.S. economy—and national security—with its relentless efforts to steal sensitive technology and proprietary information from U.S. companies, academic institutions, and other organizations, FBI Director Christopher Wray said today.

Wray described the threat from China as “diverse” and “multi-layered.” He noted that the Chinese government exploits the openness of the American economy and society.

"They've pioneered an expansive approach to stealing innovation through a wide range of actors," Wray said during opening remarks at the half-day Department of Justice China Initiative Conference in Washington, D.C.

Wray told the audience that China is targeting everything from agricultural techniques to medical devices in its efforts to get ahead economically. While this is sometimes done legally, such as through company acquisitions, China often takes illegal approaches, including cyber intrusions and corporate espionage.

"They've shown that they're willing to steal their way up the economic ladder at our expense," he said.

The FBI is using traditional law enforcement techniques as well as its intelligence capabilities to combat these threats. He said the FBI currently has about 1,000 investigations into Chinese technology theft.

> **"They've shown that they're willing to steal their way up the economic ladder at our expense."**
> FBI Director Christopher Wray

Just last month, a Harvard University professor was charged (https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/harvard-university-professor-and-two-chinese-nationals-charged-in-three-separate-china-related-cases) with lying about his contractual arrangement with China.

Wray also called for a whole-of-society response to these threats. He urged U.S. companies to carefully consider their supply lines and whether and how they do business with Chinese companies. While a partnership with a Chinese company may seem profitable today, a U.S. company may find themselves losing their intellectual property in the long run.

Additionally, U.S. universities should work to protect their foreign students from coercion from foreign governments, Wray said.

Wray noted, however, that these threats do not mean the U.S. shouldn't welcome Chinese students or visitors.

"What it does mean is that when China violates our criminal laws and well-established international norms, we are not going to tolerate it, much less enable it," he said. "The Department of Justice and the FBI are going to hold people accountable for that and protect our nation's innovation and ideas."

Resources

- Responding Effectively to the Chinese Economic Espionage Threat (https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat)

POLITICO

Grand Old Primary

POLITICO's coverage of the race for the Republican presidential nomination.

Republican presidential candidate Donald Trump speaks during a campaign stop at the Allen County War Memorial Coliseum, Sunday, May 1. | AP Photo

Trump: 'We can't continue to allow China to rape our country'

By NICK GASS | 05/02/2016 06:37 AM EDT

Donald Trump ratcheted up his language toward China on Sunday, remarking at one point

To give you the best possible experience, this site uses cookies. If you continue browsing, you accept our use of cookies. You can review our privacy policy to find out more about the cookies we use.

Accept

"Don't forget. We're like the piggybank that's being robbed. We have the cards. We have a lot of power with China," Trump told an audience in Fort Wayne, Indiana. "When China doesn't want to fix the problem in North Korea, we say, 'Sorry, folks, you gotta fix the problem.' Because we can't continue to allow China to rape our country. And that's what they're doing. It's the greatest theft in the history of the world."

But even though China, in Trump's words, is committing "rape" against the U.S., he isn't mad at the Chinese. On the contrary, he said, he is angry with U.S. leaders for allowing it to do so.

"What China has done — and I like China — I've made a lot of money with China," Trump said. "The Bank of America building in San Francisco, a building in New York, 1290 Avenue of the Americas, one of the biggest floor plates in the whole city of New York. I do great with China, I sell them condos, I have the largest bank in the world from China, the largest in the world by far. They're a tenant of mine in a building I own in Manhattan."

"I mean, China's great. No problem. I'm not angry with China," he continued. "And I'm not angry at Japan. And I'm not angry at Mexico. I'm not angry at anybody. I'm angry at our leaders, because they are grossly incompetent and they shouldn't have ever been elected to do this job. Terrible."

Railing against trade deals has long been a staple of Trump's stump speech, though he tends to emphasize the topic more often in blue-collar areas that have been hit hard by foreign competition.

Trump has often spoken about in particular about Carrier, the appliance manufacturer that recently announced it would lay off some 1,400 workers in Indianapolis as it moved operations to Mexico.

In February, a secretly filmed video showing employees shouting obscenities at a manager as he announces the layoffs went viral.

"Carrier will not leave Indiana if I'm president," Trump has said.

To give you the best possible experience, this site uses cookies. If you continue browsing, you accept our use of cookies. You can review our privacy policy to find out more about the cookies we use.

Accept

Careers

Credit Card Payments

Digital Edition

FAQ

Feedback

Headlines

Photos

POWERJobs

Press

Print Subscriptions

Write For Us

RSS

Site Map

Terms of Service

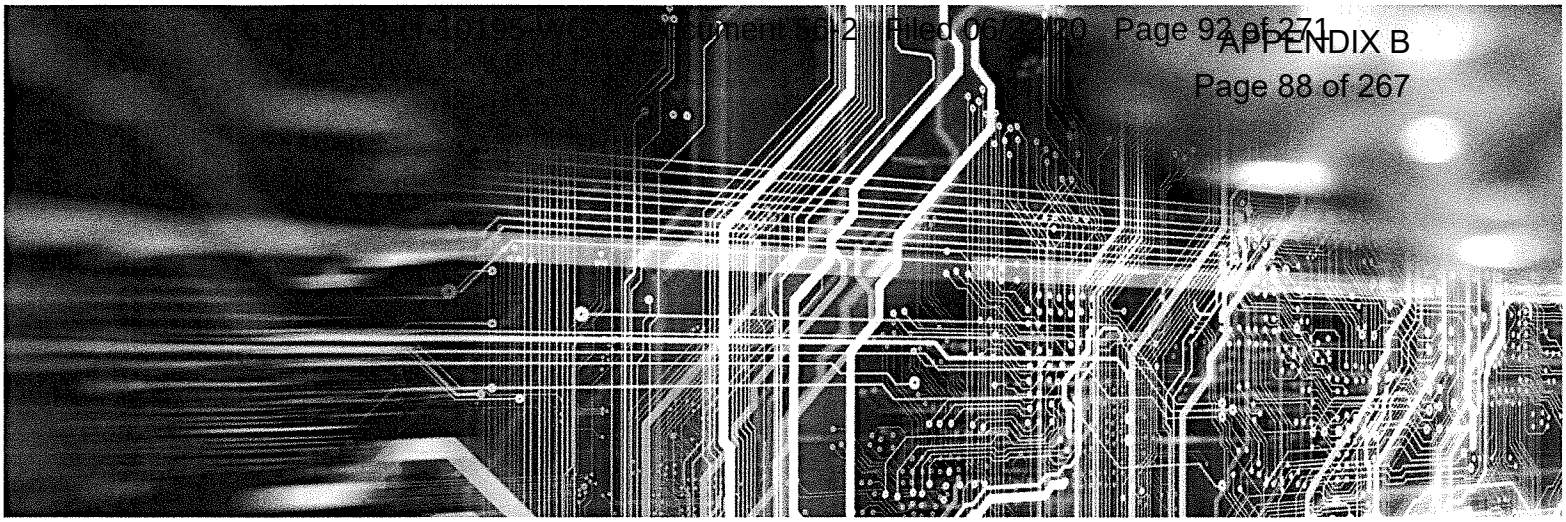
Privacy Policy

Do not sell my info

© 2020 POLITICO LLC

To give you the best possible experience, this site uses cookies. If you continue browsing, you accept our use of cookies. You can review our privacy policy to find out more about the cookies we use.

Accept



★ ★ ★

How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World

THE WHITE HOUSE

White House Office of Trade and Manufacturing Policy

June 2018

I. China's Strategies of Economic Aggression

> *The Chinese government is implementing a comprehensive, long-term industrial strategy to ensure its global dominance.... Beijing's ultimate goal is for domestic companies to replace foreign companies as designers and manufacturers of key technology and products first at home, then abroad.*
>
> *U.S.-China Economic and Security Review Commission*[1]

The People's Republic of China (China) has experienced rapid economic growth to become the world's second largest economy[2] while modernizing its industrial base and moving up the global value chain. However, much of this growth has been achieved in significant part through aggressive acts, policies, and practices that fall outside of global norms and rules (collectively, "economic aggression").[3] Given the size of China's economy and the extent of its market-distorting policies, China's economic aggression[4] now threatens not only the U.S. economy but also the global economy as a whole.

In some respects, China has been transparent about its aggressive acts, policies, and practices. They are revealed in Chinese government documents,[5] through behaviors of Chinese State actors,[6] and from reports produced by business organizations, think tanks, and government agencies.[7] Four categories of such economic aggression which are outside the scope of this report include:

- ***Protect China's Home Market From Imports and Competition:*** This category features high tariffs, non-tariff barriers, and other regulatory hurdles.[8]
- ***Expand China's Share of Global Markets***: Industrial policy tools include financial support to boost exports and the consolidation of State-Owned Enterprises into "national champions"[9] that can compete with foreign companies in both the domestic and global markets. Chinese enterprises also benefit from preferential policies that lead to subsidized overcapacity in China's domestic market, which then depresses world prices and pushes foreign rivals out of the global market.[10]
- ***Secure and Control Core Natural Resources Globally:*** China uses a predatory "debt trap" model of economic development and finance that proffers substantial financing to developing countries in exchange for an encumbrance on their natural resources and access to markets. These resources range from bauxite, copper, and nickel to rarer commodities such as beryllium, titanium, and rare earth minerals.[11] This predatory model has been particularly effective in countries characterized by weak rule of law and authoritarian regimes.[12]
- ***Dominate Traditional Manufacturing Industries:*** China has already achieved a leading position in many traditional manufacturing industries. It has done so in part through preferential loans and below-market utility rates as well as lax and weakly enforced environmental and health and safety standards.[13] As the European Chamber of Commerce has documented: "For a generation, China has been the factory of the world." By 2015, China already accounted for 28 percent of global auto production, 41 percent of global ship production, more than 50 percent of global refrigerator production, more than 60 percent

of global production of color TV sets, and more than 80 percent of global production of air conditioners and computers.[14]

In addition, China pursues two categories of economic aggression that are the focus of this report. These include:

- ***Acquire Key Technologies and Intellectual Property From Other Countries, Including the United States***
- ***Capture the Emerging High-Technology Industries That Will Drive Future Economic Growth[15] and Many Advancements in the Defense Industry***

This report will document the major acts, policies, and practices of Chinese industrial policy used to implement these two strategies.[16] Through such implementation, the Chinese State seeks to access the crown jewels of American technology and intellectual property. (A compendium of the acts, policies, and practices used to implement China's six strategies of economic aggression is presented in the Appendix.)

II. How China Seeks to Acquire Technologies and Intellectual Property and Capture Industries of the Future

Chinese industrial policy seeks to "introduce, digest, absorb, and re-innovate"[17] technologies and intellectual property (IP) from around the world.[18] This policy is carried out through: (A) State-sponsored IP theft[19] through physical theft, cyber-enabled espionage and theft, evasion of U.S. export control laws, and counterfeiting and piracy; (B) coercive and intrusive regulatory gambits to force technology transfer from foreign companies, typically in exchange for limited access to the Chinese market; (C) economic coercion through export restraints on critical raw materials and monopsony purchasing power; (D) methods of information harvesting that include open source collection; placement of non-traditional information collectors at U.S. universities, national laboratories, and other centers of innovation; and talent recruitment of business, finance, science, and technology experts; and (E) State-backed, technology-seeking Chinese investment.

A. Physical Theft and Cyber-Enabled Theft of Technologies and IP

The Office of the Director of National Intelligence notes: "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[20] Strategic sectors in emerging industries known to have been targeted include "electronics, telecommunications, robotics, data services, pharmaceuticals, mobile phone services, satellite communications and imagery, and business application software."[21]

1. Physical Theft of Technologies and IP Through Economic Espionage

Physical theft through economic espionage by company insiders or others who have trusted access to trade secrets and confidential business information provides China with a significant means to acquire U.S. technologies and intellectual property. In describing China's use of economic espionage as part of a broader strategy to acquire U.S. technology companies, the U.S.-China Economic and Security Review Commission observes:

China appears to be conducting a campaign of commercial espionage against U.S. companies involving…human infiltration to systematically penetrate the information systems of U.S. companies to steal their intellectual property, devalue them, and acquire them at dramatically reduced prices.[22]

A report from the Department of Defense's Defense Innovation Unit Experimental[23] (hereinafter the DIUx Pentagon Report) states that "the scale of the [Chinese economic] espionage … continues to increase."[24] Law enforcement efforts alone cannot keep up with (or adequately deter) a state-sponsored campaign of theft. In part, this is because U.S. companies may be unaware of theft by an insider before it is too late. In part, this is because some U.S. companies are unwilling to report the theft for fear of the adverse consequences that such a disclosure could entail. Even when victims report, the Chinese government is typically unwilling to cooperate, making a successful cross-border investigation difficult.

Open source reporting indicates China's Ministry of State Security deploys no less than 40,000 intelligence officers abroad and maintains more than 50,000 intelligence officers in mainland China.[25] This force is bolstered by hundreds of thousands of People's Liberation Army (PLA) staff members and scientists.[26]

2. Cyber-Enabled Espionage and Theft

> *Cyber tools have enhanced the economic espionage threat, and the IC [Intelligence Community] judges [that] the use of such tools is already a larger threat than more traditional espionage methods.*
>
> *Report to Congress on Foreign Economic Collection and Industrial Espionage, Office of the National Counterintelligence Executive*[27]

China engages in widespread cyber-economic campaigns involving cyber-enabled espionage to infiltrate foreign companies for the purpose of stealing intellectual property, trade secrets, business processes, and technologies.[28] Estimates of the cost of trade secret theft alone range "between $180 billion and $540 billion annually."[29] As the U.S. Trade Representative (USTR) notes:

> *For over a decade, the Chinese government has conducted and supported cyber intrusions into U.S. commercial networks targeting confidential business information held by U.S. firms. Through these cyber intrusions, China's government has gained unauthorized access to a wide range of commercially valuable business information, including trade secrets, technical data, negotiating positions, and sensitive and proprietary internal communications. These acts, policies, or practices by the Chinese government are unreasonable or discriminatory and burden or restrict U.S. commerce.*[30]

In a 2012 study of cyber intrusions, Verizon, in cooperation with 19 contributing private organizations and government agencies, analyzed over 47,000 security incidents that resulted in 621 confirmed data disclosures and at least 44 million compromised records. Of the data disclosures that focused on economic espionage (as opposed to financially motivated incidents), 96% of the cases were attributable to "threat actors in China."[31]

In 2013, the cyber-security firm Mandiant described a People's Liberation Army cyber command "fully institutionalized" within the Chinese Communist Party and staffed by more than 100,000 personnel.[32] In May of 2014, the U.S. Department of Justice (DOJ) unsealed criminal charges against five officers of the PLA for cyber-enabled economic espionage, among other hacking-related charges, related to the theft of intellectual property, trade secrets, and other sensitive business information from U.S. entities in the energy and steel industries.[33]

In September of 2015, President Barack Obama and President Xi Jinping of China formally committed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[34] According to the U.S.-China Economic and Security Review Commission 2016 Annual Report to Congress:

> *[A]lthough the number of incidents of Chinese cyber espionage detected by FireEye [a cybersecurity firm] has declined, this likely reflects a shift within China away from prolific amateur attacks toward more centralized, professionalized, and sophisticated attacks by a smaller number of actors, rather than a trend toward the cessation of Chinese cyber espionage.*[35]

3. Evasion of U.S. Export Control Laws

Closely related to China's espionage campaigns are China's State-backed efforts to evade U.S. export control laws. These laws have been put in place for national security purposes under the Arms Export Control Act (AECA)[36] and the International Emergency Economic Powers Act (IEEPA);[37] they are designed to prevent the export of sensitive technologies with military applications.

A significant problem facing the U.S. departments and agencies implementing these export controls (principally the Departments of Commerce, Defense, and State) [38] is the growth in "dual-use" technologies, which have both military and civilian utility. For example, aero-engine technologies have an obvious commercial application. When acquired by a strategic economic and military competitor like China, commercial items can be exploited for military purposes.

As an example of China's evasion of U.S. export control laws, consider the case of Amin Yu, a Chinese national who became a lawful permanent U.S. resident. As described by Assistant U.S. Attorney Daniel Irick, "Yu was part of a conspiracy that involved shell companies, off-shore accounts and false documents" and "was involved in $2.6 million in illegal transactions."[39]

From 2002 to 2012, Yu admitted in a plea bargain that "at the direction of co-conspirators working for Harbin Engineering University (HEU), a state-owned entity in the People's Republic of China, Yu obtained systems and components for marine submersible vehicles from companies in the United States. She then illegally exported those items to the PRC for use by her co-conspirators in the development of marine submersible vehicles–unmanned underwater vehicles, remotely operated vehicles, and autonomous underwater vehicles–for HEU and other state-controlled entities."[40]

4. Counterfeiting and Piracy

Counterfeiting entails the practice of producing unauthorized fake goods. Piracy is copyright infringement on a commercial scale and "consists in making an unauthorized exact copy–not a simple imitation–of an item covered by an intellectual property right."[41] China is the world's largest source of counterfeit and pirated products.[42]

Estimates of the cost of China's counterfeiting and piracy run into the hundreds of billions of dollars per year. For example, the non-partisan and independent Commission on the Theft of Intellectual Property estimates "that the annual cost to the U.S. economy continues to exceed $225 billion in counterfeit goods, pirated software, and theft of trade secrets and could be as high as $600 billion," "IP theft by thousands of Chinese actors continues to be rampant," and China "remains the world's principal IP infringer."[43]

5. Reverse Engineering

Reverse engineering in China is widespread and entails the process of disassembling and examining or analyzing a product or component for the purpose of cloning or producing something similar without authorization from the rights holder. Reverse engineering can be legal; it is illegal when the unauthorized production is of technology under patent or other IP protection.

Reverse engineering allows Chinese engineers and scientists to recreate the products of non-Chinese companies and thereby forego the time and cost of research and development. The practice of reverse engineering is consistent with China's industrial policy goal to introduce, digest, and absorb a foreign technology and "re-innovate" that technology with improvements.[44]

B. Coercive and Intrusive Regulatory Gambits to Force Technology and IP Transfer

> *[A] longstanding feature of China's industrial policy is that foreign companies are often pushed to transfer technology as the price of market entry, which is in contravention of its commitments as a member of the World Trade Organisation (WTO) . This situation is exacerbated by the fact that the Chinese authorities' ultimate aim is to absorb these technologies...as domestic companies begin to catch up technologically, market access for foreign companies will become increasingly difficult.*
>
> *European Chamber of Commerce*[45]

Chinese industrial policy features a wide range of coercive and intrusive regulatory gambits to force the transfer of foreign technologies and IP to Chinese competitors, often in exchange for access to the vast Chinese market. In its 2017 Member Survey, the U.S.-China Business Council reports that "tech transfer to gain market access is an acute issue for those who face it; nearly 20 percent of respondents to a U.S.-China Business Council 2017 Member Survey have been asked to transfer technology during the past three years" and that "ninety-four percent remain concerned about IP protection."[46]

China's instruments of coercion to force the transfer of foreign technologies and IP to Chinese competitors include: (1) foreign ownership restrictions such as forced joint ventures and partnerships that explicitly or tacitly require or facilitate technology transfers; (2) adverse administrative approvals and licensing processes; (3) discriminatory patent and other IP rights restrictions; (4) security reviews; (5) secure and controllable technology standards; (6) data localization; (7) burdensome and intrusive testing; (8) discriminatory catalogues and lists; (9) government procurement restrictions; (10) imposition of indigenous technology standards that deviate significantly from international norms and that may provide backdoor Chinese access to source codes; (11) forced research and development ("R&D localization); (12) antimonopoly laws; (13) Expert Review Panels; (14) Chinese Communist Party Committees that influence corporate governance; and (15) placement of Chinese employees at foreign joint ventures.

1. Foreign Ownership Restrictions

China uses foreign ownership restrictions[47] to force or induce the transfer of technology and IP, often as a condition of access to the Chinese market.[48] Such investment restrictions may also serve both to deter entry of foreign producers into the Chinese market and to enhance indigenous innovation and import substitution.

For example, China requires foreign companies to enter into joint ventures or partnerships with minority stakes in exchange for access to the Chinese market in select sectors.[49] As noted by the USTR: "These requirements prohibit foreign investors from operating in certain industries unless they partner with a Chinese company, and in some cases, unless the Chinese partner is the controlling shareholder."[50]

Once a U.S. or foreign company is coerced into entering a joint venture with a Chinese partner, it opens itself up to the transfer of technology and IP. This can happen through the joint manufacturing process. It can also happen when the Chinese partner engages in covert actions to steal the foreign IP or technology using its access and proximity to the foreign enterprise.

As foreign pressure mounts to end coercive foreign ownership restrictions, China increasingly relies on *tacit* coercion and minimizes written records of forced technology transfer requirements in particular deals.[51] Despite repeated promises from top Chinese leaders to end this practice, it continues.[52]

2. Adverse Administrative Approvals and Licensing Requirements

> *The Chinese government uses its administrative licensing and approvals processes to force technology transfer in exchange for the numerous administrative approvals needed to establish and operate a business in China.*
>
> *U.S. Trade Representative*[53]

Foreign companies seeking to invest in China must obtain a variety of administrative approvals; these include investment approvals, project approvals, local approval for site-related conditions, and national security approvals, among others. At each stage, Chinese regulators may seek to extract concessions or force the transfer of technology or IP. In these ways, China's extensive,

burdensome, opaque, and discriminatory approvals process functions as a significant non-tariff barrier to entry and a coercive tool to force the transfer of technologies and IP.

China imposes licensing requirements on more than 100 different business activities, e.g. food and drug production, mining, and telecommunications services. In the course of an often vague, ambiguous, and discretionary licensing process, China can extract valuable intellectual property, acquire proprietary information about marketing channels, and press for more favorable, below-market commercial terms for the local partner(s). These licensing requirements also raise the costs of foreign competitors and can induce delays entering the Chinese market.

3. Discriminatory Patent and Other IP Rights Restrictions

China seeks to force foreign patent and technology holders to accept below-market royalty rates in licensing and other forms of below-market compensation for their technologies.[54] China also seeks to otherwise restrict the IP rights of foreigners in at least three ways.

First, China maintains special rules for foreign companies that license technologies to domestic companies. These rules mandate that all improvements to a technology belong to the party making the improvements and provide that the foreign licensor cannot stop the Chinese licensee from making improvements to the technology.[55] As noted by the USTR: "These provisions are particularly harmful to a U.S. licensor if the Chinese licensee makes an improvement severable from the original invention and then patents the severable improvement in China or elsewhere."[56]

Second, China seeks to limit the time that a foreign patent or rights holder has exclusive control over the technology or patent in licenses with domestic parties. For example, as part of its restrictions on foreign joint venture (JV) partners, the USTR notes: "[T]he term of the technology transfer agreement to the JV shall 'generally not exceed ten years.' The provision may result in U.S. companies only having control over their transferred technology for ten years, even though some forms of technology, such as patents and trade secrets, may be protectable for much longer than ten years."[57]

Third, China seeks to extend the right to use a foreign technology in perpetuity after the licensing or use term expires. As noted by the USTR in the joint venture context: "After the conclusion of the JV-related technology transfer agreement [under the relevant Chinese regulations,] the technology importing party shall have the right to continue using the technology…This means that under the JV Regulations, the Chinese joint venture licensee has the right to use the U.S. licensor's technology in perpetuity."[58]

These market-distorting practices undermine the ability of U.S. firms to compete in China and continue investment in innovation. These practices also provide Chinese firms with an advantage in global markets over foreign competitors that must pay full royalty and other rates while depriving foreign technology owners of a fair return. In these ways, China's discriminatory and restrictive policies on patent and other IP rights further China's goal of indigenous innovation through re-innovation while truncating the intellectual property rights of foreigners.

4. Security Reviews Force Technology and IP Transfers

China uses security reviews to force foreign enterprises to disclose proprietary information.[59] At risk are source codes, encryption algorithms, and other sensitive IP.

Chinese use of security reviews dates back to older laws like China's 1999 "Commercial Encryption Regulation," which classified encryption as a state secret. In recent years, China has increased its use of security reviews to target emerging high-technology industries.

China's *Cybersecurity Law*,[60] which entered into force in June 2017, establishes security reviews for products and services, imposes restrictions on the cross-border flow of data, requires data localization, and authorizes the development of national cybersecurity standards that exceed the burden and scope of international standards.

The European Chamber of Commerce has expressed concern that as the *Cybersecurity Law* is implemented, it is likely that "companies will have to submit information on their products' design and source codes to government-affiliated review organisations."[61] Similarly, the USTR has warned: "Companies may be forced to disclose critical technologies, including source code, complete design databases, behavior models, logic models, and even floor plans and physical layouts of central processing units."[62]

5. Secure and Controllable Technology Standards

China continues to codify into law "secure and controllable" technology standards through laws such as the National Security Law, the Cyber Security Law, the National Cyber Security Standard, and the Technical Committee Standards. It "has more than 30 such measures in various industries."[63]

Conformance with the secure and controllable technology standards (also known as "secure and trustworthy" and "indigenous and controllable") requires foreign firms to "surrender key technologies to Chinese authorities, such as source code and encryption algorithms"[64] and submit to "extensive IP disclosures."[65] The secure and controllable technology standards thereby act as a barrier to entry to firms reluctant to surrender their technologies and IP and as a coercive tool to force technology and IP transfer, thereby promoting indigenous innovation.

6. Data Localization Mandates

China is increasingly attempting to force foreign enterprises to localize valuable data or information within China, e.g., store their data and information on servers in China.[66] This practice of data localization can act as a barrier to entry for foreign companies unwilling to share their data because of the high risk such data localization poses in China. As the U.S. Chamber of Commerce notes:

> *[I]f a foreign company is forced to localize a valuable set of data or information in China, whether for R&D purposes or simply to conduct their business, it will have to assume a significant amount of risk that its data or information may be misappropriated or misused, especially given the environment in China, where companies face significant legal and other uncertainties when they try to protect their data and information.*[67]

7. Burdensome and Intrusive Testing

China imposes burdensome and intrusive testing requirements that extend beyond the need for public health and safety to force foreign companies to reveal trade secrets, source code, encryption algorithms, and other sensitive IP. For example, China's Compulsory Certification program requires foreign producers to undergo extensive and redundant in-country tests and factory inspections and to be certified before legally marketing certain products in China. Product types in the current catalogue[68] include agricultural machinery, electric tools, motor vehicles and parts, medical devices, and firefighting equipment.[69]

Besides forcing technology transfer, burdensome and intrusive testing deters market entry and raises the costs of foreign competitors operating in the domestic market, thereby offering protection to domestic producers.

8. Discriminatory Catalogues and Lists

China's system of ministerial and provincial catalogues and lists can raise customs barriers, deter market entry, further expand licensing requirements, tighten foreign investment restrictions, and force technology transfer. For example, the *Catalogue of Telecommunications Services*[70] has expanded the scope of telecommunications services subject to licensing requirements. Only foreign companies participating in a joint venture with a Chinese company can hold a license. Absent a license, a foreign company cannot use its brand or trademark when selling or supplying services through its joint venture.[71]

Similarly, when a foreign company's products are excluded from an approved list in a Chinese government catalogue, the foreign company may be denied benefits available to domestic competitors such as preferential tax rates and low-interest loans from Chinese banks available to its Chinese competitors.

In these ways, China's catalogues and lists serve as significant non-tariff barriers to entry and as industrial policy tools to force the transfer of technologies and intellectual property while providing preferential treatment to domestic competitors.[72]

9. Government Procurement Restrictions

China maintains an expansive set of government procurement restrictions to promote import substitution and indigenous innovation. As the European Chamber of Commerce notes: "China is not a party to the plurilateral Agreement on Government Procurement (GPA) under the WTO, and its public procurement market remains largely closed to foreign suppliers…government procurement has been observed to favour domestic producers."[73]

Catalogues and lists often reinforce China's procurement restrictions. So, too, do discriminatory reimbursement schemes for foreign products, e.g., pharmaceuticals.

10. Indigenous Technology Standards That Deviate from International Norms

> *China sometimes formulates national standards in strategic industries that deliberately differ from international standards in order to impede market access for foreign technology and to favour Chinese technology on the domestic market. Examples of Chinese national standards are the FDD-LTE standard for 4G mobile networks, the WAPI standard for wireless networks and independent standards for electric vehicle charging stations. If such a national path of standardisation also manifests itself in smart manufacturing, market access for foreign tech suppliers could be considerably restricted.*
>
> *Mercator Institute for China Studies*[74]

China imposes unique, indigenous technical standards that lack harmonization with, and deviate significantly from, international standards. Target industries include aviation, computer numerical control devices, machine tools, medical tools, and robotics.[75]

These indigenous standards can serve as a tool to pressure foreign companies to reveal their source code, encryption codes, and other technologies and IP. These indigenous standards can be "confusing" and "unnecessarily duplicative" while creating trade barriers that restrict market entry and foreign imports."[76] They help drive those companies implementing the standards towards Chinese technology suppliers rather than U.S. and foreign suppliers while protecting Chinese brands and promoting indigenous innovation. In addition, they may provide backdoor Chinese access to source codes.[77]

China's indigenous technology standards also potentially "serve to reduce the licensing fees that Chinese companies would have to pay to use foreign technologies in industries covered [by China 2025]."[78] China "aims to spread Chinese standards abroad, particularly in countries linked to its One-Belt One-Road—a Chinese initiative to connect Eurasian economies through infrastructure, trade, and investment."[79]

11. Forced Research & Development ("R&D Localization")

> *The CEO of a large multinational telecommunications equipment company recently shared with ITIF [Information Technology & Innovation Foundation] that he opened up a large R&D facility in Beijing that employs over 500 scientists and engineers. When asked if he did this to access Chinese engineering talent, he responded bluntly: 'Unless I promised the Chinese Government that I would open up an advanced technology lab there, I was told that I would not be able to sell to the Chinese telecommunications providers'...*
>
> *United States Trade Representative*[80]

China uses a variety of methods to force the placement of foreign research and development facilities in China as a condition of access to the Chinese market ("R&D localization").[81] For example, China issued new market access rules in 2017. The U.S. Trade Representative states: "These rules require that NEV manufacturers 'master' the development and manufacturing technology for a complete NEV, rather than just one of the three key technologies listed in the

2009 market access rules, and possess key R&D capacities."[82] China's 2014 Integrated Circuits Guidelines also call for establishing R&D, along with manufacturing and operating centers in China.[83] One motive for China's acquisition of U.S. companies is to capture their R&D facilities.[84]

12. Antimonopoly Law Extortion

China uses the *Antimonopoly Law of the People's Republic of China* not just to foster competition but also to force foreign companies to make concessions such as reduced prices and below-market royalty rates for licensed technology.[85] These concessions provide Chinese enterprises with a competitive advantage in the home market and global markets.

China's ability to extort concessions lies in its authority to impose fines of between one and ten percent of a foreign company's revenues for the previous year for alleged anti-competitive practices. As an example, San Diego-based Qualcomm agreed to a fine of $975 million; it also was forced to accept below-market royalty rates on patents used by Chinese smartphone manufacturers.[86]

13. Expert Review Panels Force Disclosure of Proprietary Information

Numerous Chinese administrative agencies empower Expert Review Panels composed of government, industry, and academic representatives as part of their review and approvals processes. These panels have broad powers to extract proprietary information from foreign companies under the guise of normal review[87] and thereby may help induce the transfer of technologies, IP, business processes, trade secrets, and other proprietary information. As an additional risk factor, members of these panels may have a competitive interest in the information that may be disclosed.[88]

14. Chinese Communist Party Co-opts Corporate Governance

The *Company Law of the People's Republic of China* authorizes the establishment of Communist Party committees in companies that are not State-owned "to carry out the activities of the party in accordance with the charter of the Communist Party of China."[89] Following a dictate from President Xi Jinping,[90] both Chinese State-Owned Enterprises and the joint venture partners of foreign companies are now increasingly including Chinese Communist Party Committees in corporate charters and in their corporate governance decisions.[91] In these ways, corporate governance has become a tool to advance China's strategic goals, rather than simply, as is the custom of international rules, to advance the profit-maximizing goals of the enterprise.

Under the Xi revision, boards of directors may now receive guidance directly from the Chinese Communist Party.[92] For example, China's Internet national champion Baidu has a Party Committee that links Baidu's corporate operations with Chinese industrial policy and China's political goals.[93] Baidu has been particularly active in Silicon Valley and with its U.S. investments in artificial intelligence and autonomous driving technologies.[94]

Most broadly, the number of Communist Party committees in private enterprises has increased in recent years.[95]

15. Placement of Chinese Employees with Foreign Joint Ventures

After China successfully forces a foreign company to enter into a joint venture, it may recruit employees for the JV that work in the Chinese partner's facilities. As the USTR notes: "The risk of technology loss is exacerbated when the Chinese partner in the JV operation maintains other factories and workers that compete with the JV operation. The employees of the JV often are recruited from, or have ties to, the Chinese partner's existing operations. Under these conditions, there is a considerable likelihood that the JV's technology and knowhow will leak, either through 'unintentional osmosis or through intentional diversion.'"[96]

C. Economic Coercion to Force Technology and IP Transfer

> *Chinese export restrictions offer a competitive advantage to Chinese industries that benefit from lower input prices. At times, non-Chinese buyers have been forced to buy their raw materials at a price that is more than twice as high as that paid by Chinese firms. In some cases, these raw materials can amount to a considerable share of the total production cost. Rare earths represent, for example, more than 50% of cost for wind turbine components and 50% to 60% for a LCD display. Therefore, the price difference can carry a decisive competitive disadvantage for components' makers outside China.*
>
> *European Commission*[97]

1. Export Restraints Restrict Access to Raw Materials

China has a commanding share of a wide range of critical raw materials[98] essential to the global supply chain and production of high-technology and high value-added products. For example, China is the world's dominant producer of rare earths, tungsten, and molybdenum.[99]

China has used export restraints, including export quotas and export duties, to restrict access to critical raw materials. As the USTR notes:

> *China's export restraints affect U.S. and other foreign producers of a wide range of downstream products, such as steel, chemicals, hybrid and electric cars, energy efficient light bulbs, wind turbines, hard-disk drives, magnets, lasers, ceramics, semiconductor chips, refrigerants, medical imagery, aircraft, refined petroleum products, fiber optic cables and catalytic converters. The export restraints can create serious disadvantages for these foreign producers by artificially increasing China's export prices for their raw material inputs, which also drives up world prices.... The export restraints can also create pressure on foreign downstream producers to move their operations, technologies and jobs to China.*[100, 101]

2. Monopsony Purchasing Power

China's State-Owned Enterprises have significant monopsony purchasing power in select markets, e.g., aviation.[102] China seeks to use its significant purchasing power in select markets to extract concessions from foreign sellers. Concessions may include increased localized production and the forced transfer of foreign technology. Exercising this monopsony power can strengthen the Chinese manufacturing base and supply chain, particularly in the high-technology space.

D. Information Harvesting

China acquires U.S. technologies and IP from America's national security innovation base through three primary channels of information harvesting.

1. Open Source Collection of Science and Technology Information

Large cadres of Chinese State actors engage in systematic, large-scale, open-source collection operations. They exploit foreign science and technology information to acquire foreign technologies and intellectual property and thereby gain competitive advantage by circumventing the costs and risks of indigenous research.[103]

Although many other countries and the citizens of countries leverage open sources to advance technology, particularly in the age of the Internet, what differentiates China is the historical scale and scope of the institutionalization of open source collection as a means of acquiring the world's technologies and IP. The DIUx Pentagon Report indicates that China makes "maximum use of diversified sources: scanning technical literature, analyzing patents, reverse engineering product samples and capturing conversations at scientific meetings."[104]

In 1985, there were more than 400 major science and technology institutes in China employing more than 60,000 workers "investigating, collecting, analyzing, synthesizing, repackaging, benchmarking, and reverse engineering."[105] Today, the Institute of Scientific and Technical Information of China is one such institute, with a "mandate" to provide "comprehensive information services to industry, universities, research institutes, and research personnel," a staff team of over 500, and a record of collecting millions of doctoral theses and government reports and hundreds of thousands of reference books along with thousands of foreign journals, monographs, and conference proceedings.[106]

In 1991, veteran Chinese spies published *Sources and Methods of Obtaining National Defense Science & Technology Intelligence*,[107] a textbook known as China's open source collection "Spy Guide."[108] It references how open source collection is a Chinese State activity designed to further strategic goals and notes how open source collection has evolved into a "profession within the broader field of S&T [Science and Technology]."[109] Excerpts from the guide include: "Information is documents." "Information is not intelligence. Information is the source of intelligence;" "Collection policy is determined according to the intentions of the higher authorities;" and "The first thing that must be known when setting collection policy is where the intelligence elements fit into the national intelligence system.[110]

The DIUx Pentagon Report describes this document as "a comprehensive account of China's foreign military open-source collection…collecting all types of media (including verbal information prized for its timeliness over written information) and making them available in database form."[111] Open source reporting credits the acquisition of foreign technological information through open source collection "with reducing research costs by 40 to 50 percent and time by 60 to 70 percent."[112]

2. Chinese Nationals In the U.S. as Non-Traditional Information Collectors[113]

More than 300,000 Chinese nationals annually attend U.S. universities or find employment at U.S. national laboratories, innovation centers, incubators, and think tanks. Chinese nationals now account for approximately one third of foreign university and college students in the United States and about 25 percent of graduate students specializing in science, technology, engineering, or math (STEM).[114]

Non-military sectors and institutions increasingly and routinely generate scientific and technological advancements with dual-use applications. Aware that Chinese nationals attending U.S. universities or finding employment at U.S. national laboratories, innovation centers, incubators, and think tanks may have access to cutting-edge information and technologies, the Chinese State has put in place programs aimed at encouraging Chinese science and engineering students "to master technologies that may later become critical to key military systems."[115] The national and economic security risks are that the Chinese State may seek to manipulate or pressure even unwitting or unwilling Chinese nationals into becoming non-traditional information collectors that serve Beijing's military and strategic ambitions.

During a February 2018 U.S. Senate Intelligence Committee hearing,[116] Senator Marco Rubio (R-FL) asked FBI Director Christopher Wray what the "counterintelligence risk posed to U.S. national security" was from "Chinese students, particularly those in advanced programs in sciences and mathematics?" Wray responded that the FBI has observed "the use of nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students…in almost every… field office that the FBI has around the country. It is not just in major cities, it's in small ones as well. It's across basically every discipline; and I think the level of naiveté on the part of the academic sector about this creates its own issues."

In FBI Director Wray's view, Chinese non-traditional collectors "are exploiting the very open research and development environment that we have, which we all revere. But they're taking advantage of it, so one of the things we're trying to do is view the China threat as not just the whole-of-government threat, but a whole-of-society threat on their end, and I think it's going to take a whole-of-society response by us." As the DIUx Pentagon Report notes:

> *Academia is an opportune environment for learning about science and technology since the cultural values of U.S. educational institutions reflect an open and free exchange of ideas. As a result, Chinese science and engineering students frequently master technologies that later become critical to key military systems, amounting over time to unintentional violations of U.S. export control laws.*[117]

State-backed Chinese enterprises increasingly finance joint research programs and the construction of new research facilities on U.S. campuses. For example, Huawei is a company founded by a former Chinese military officer that raises national security concerns.[118] Section 1656 of the Fiscal Year 2018 National Defense Authorization Act prohibits the Department of Defense from procuring or obtaining "covered telecommunications or services" and names Huawei in the definition of covered transactions.[119]

Huawei has partnered with the University of California-Berkeley on research focusing on artificial intelligence and related areas such as "deep learning, reinforcement learning, machine learning, natural language processing and computer vision," [120] areas which all have important future military applications.

Chinese State actors are strategically building research centers in innovation centers and hubs like Silicon Valley and Boston. For example, the Chinese Internet firm Baidu has "set up the Institute for Deep Learning in Silicon Valley so it could compete with Google, Apple, Facebook and others for talent in the artificial intelligence field." [121]

At the national laboratory level where leading edge defense research takes place, open source reporting indicates Chinese nationals working at top laboratories such as Los Alamos in New Mexico and Livermore in California have returned to China with expertise and knowledge transferrable to the development of systems with military applications.[122] Examples cited include hypersonic glide vehicles, which travel at speeds in excess of Mach 5 and "are specifically designed for increased survivability against modern ballistic missile defense systems."[123]

3. Recruitment of Science, Technology, Business, and Finance Talent

China State actors recruit scholars, researchers, technology experts, and scientists at the forefront of their respective fields across the world. Such talent recruitment also targets the top employees of companies that a Chinese enterprise may seek to acquire, partner with, or invest in.

China's talent recruitment strategically complements China's efforts to target emerging high-technology industries and involves well-established Chinese government programs and large, stable funding streams. It focuses on two main categories of recruitment–non-Chinese talent and Chinese talent.

Non-Chinese talent recruitment targets academic and industry leaders from research institutes, laboratories, and universities in other countries. Inducements include financial and material benefits such as favorable taxation policies, free housing, insurance, family settlement funds, research funding, prestigious appointments, and government awards.[124] In serving the Chinese State, this non-Chinese talent fills knowledge gaps for civilian, military, and dual-use technologies.

Chinese talent recruitment includes nationals studying or working abroad. Chinese recruiters appeal to national pride and urge a "return to China" to "serve the Motherland."[125] Those who return are rewarded with financial incentives and career opportunities. Those staying abroad are afforded multiple avenues to "serve the country,"[126] often including short-term visits to China and drafting reports outlining their research abroad.[127]

For example, the "Thousand Talents Plan," a recruitment program launched in 2008 by the central government of China, targets scholars who are leaders in their respective fields with top-level research capabilities, and who may hold intellectual property rights, key technologies, or patents in technological fields desired by China. These recruits may receive lucrative and prestigious positions at premier Chinese research institutes, labs, or universities.[128]

Chinese government sources claim over 44,000 highly skilled Chinese personnel have returned to China since 2009 through talent plans.[129] As noted by *China Daily*, which is owned by the Chinese Communist Party: "China has more than 300 entrepreneurial parks for students returned from overseas. More than 24,500 enterprises have been set up in the parks by over 67,000 overseas returnees."[130]

E. Technology-Seeking, State-Financed Foreign Direct Investment

> *The Chinese government directs and unfairly facilitates the systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies, to obtain cutting-edge technologies and intellectual property and generate large-scale technology transfer in industries deemed important by state industrial plans.*
>
> *United States Trade Representative*[131]

The Chinese government has institutionalized the industrial policy of inducing investment in "encouraged" high-technology sectors[132] using the financial resources and regulatory instruments of the State.[133] China's government has a multi-billion dollar set of State-backed funds[134] that contribute to technology investment and uses an array of State actors to implement its strategies of acquiring foreign technologies and intellectual property.

From 2006 to 2014, much of China's outbound foreign direct investment (FDI) focused on the acquisition of core natural resources. However, since 2015, China has increasingly directed capital to acquire high-technology areas of the U.S. economy in particular.

In policy documents such as *Made in China 2025,*[135] China has articulated the target list of technology sectors it seeks to dominate.[136] Much of recent Chinese investment behavior appears consistent with this target list.

For example, since 2012, CB Insights has catalogued more than 600 high-technology investments in the United States worth close to $20 billion conducted by China-based investors, with artificial intelligence, augmented and virtual reality, and robotics receiving particular focus.[137] China's biggest sovereign wealth fund, the China Investment Corporation, has used a significant fraction of the $800 billion of assets under management[138] for a venture fund focusing on Silicon Valley.[139]

1. Chinese State Actors Involved in Technology-Seeking FDI

Chinese State actors involved in technology-seeking FDI include: (a) State-Owned Enterprises (SOEs); (b) private Chinese companies with interlocking ties to the Chinese State; and (c) State-backed investment funds.

a. Chinese State-Owned Enterprises (SOEs)

> *President Xi Jinping stressed the Communist Party of China's (CCP) unswerving leadership over State-Owned Enterprises (SOEs) during a national meeting on building the role of the Party within SOEs.... Efforts should be made to strengthen and improve Party leadership, as well as to build the role of the Party in SOEs to make them the most trustworthy and reliable forces of the CCP and the state, said Xi.... SOEs should also become important forces to implement decisions of the CCP Central Committee.... Describing SOEs as an important material and political basis for socialism with Chinese characteristics and an important pillar and reliable force for the CCP's governance of the country, Xi said Party leadership and building the role of the Party are 'the root and soul' for SOEs.*
>
> *Xinhua*[140]

President Xi Jinping's address to a national meeting underscores the important role SOEs play in Chinese industrial policy. SOEs are the most visible symbols of China's non-market economy.[141] A significant share of China's non-financial outbound FDI is driven by SOEs.[142] SOEs account for roughly a third of outbound non-financial FDI.[143]

Besides the economic and national security risks associated with the strategic assets and military-capable technologies of the United States being acquired by the SOEs of a strategic competitor like China, the U.S.-China Economic and Security Review Commission notes an additional legal complication: "Some Chinese SOEs are evading [civil] legal action in the United States by invoking their status as a foreign government entity under the Foreign Sovereign Immunities Act."[144]

b. Private Chinese Companies Guided By the Chinese State

> *The Chinese government maintains significant influence over private firms' investment decisions—including encouraging, modifying, or banning deals based on the specific industries, geographies, and technologies involved—by utilizing a mix of financial incentives, political arrangements, and agreements among company shareholders.*
>
> *U.S.-China Economic and Security Review Commission*[145]

This observation is supported by four characteristics of Chinese enterprise. First, many enterprises in China depend on financing from the Chinese State, often at preferential rates.

Second, China can influence private enterprises through the aforementioned rules China has put in place with respect to the Chinese Communist Party's mandated role in corporate governance.

Third, China's executive ranks are populated with current or former members of the Chinese Communist Party or government. As Columbia Law School professors Wentong Zheng and Curtis Milhaupt found: "95 out of the top 100 private Chinese firms by revenue and eight out of the top ten Internet firms by revenue were founded or are controlled by a current or former member of a central or local political organization such as the People's Congresses and People's Political Consultative Conferences."[146]

According to its 2017 Member Survey, the U.S.-China Business Council finds that the "challenges of competition with Chinese companies has been a top concern for USCBC members for many years" and that "competition concerns are not unique to having state-owned enterprise rivals. Most companies are competing with private, non-state-owned companies in China (and other foreign companies), in addition to SOEs."[147] As noted above, the Chinese government has significant influence over many of these putatively private companies.

Advantages that accrue to Chinese competitors cited by the 2017 Member Survey include preferential government financing (63 percent), preferential licensing and approvals (58 percent), preferential access to government contracts (53 percent), tax benefits (45 percent), and lower land costs (40 percent).[148]

Fourth, sector-based restrictions on China's outbound foreign direct investment guide investment flows from private Chinese companies into strategic sectors. For example, as of April 2018, guidance published by the Chinese government divided outbound investment flows into the categories of encouraged, restricted, and prohibited. The encouraged category includes investments that promote the acquisition of advanced technology while the restricted category includes sectors like real estate that do not rely on technology.[149]

These sector-based restrictions thereby strategically align the deployment of capital abroad by private Chinese companies with the priorities of the Chinese State rather than with the principles of economic efficiency and profit maximization that normally guide private sector investment in market economies and in the international system.

c. *State-Backed, Technology-Seeking Investment Funds*

China relies significantly on sovereign wealth funds (SWF) and other government-backed investment vehicles to finance its outbound foreign direct investment. This trend started in 2007 with the formation of the China Investment Corporation, which now has under management close to one trillion dollars.[150]

Three of the world's ten largest SWFs are from China. According to the Mercator Institute, "while these funds and their management often present themselves as private enterprises, the state's active role is concealed behind an opaque network of ownership and funding structures."[151]

China's targeting of the integrated circuit industry illustrates how China's State-backed funds can rapidly deploy to acquire foreign assets. In June 2014, China's Ministry of Industry and Information Technology (MIIT) announced the National Guideline for the Development and Promotion of the Integrated Circuit Industry. This National Guideline detailed the Chinese government's goals for creating a self-sufficient integrated circuit sector that meets industrial and security requirements.[152]

Ninety days after issuance of the National Guideline, MIIT announced the formation of its National IC Industry Investment Fund to mobilize capital.[153] This fund is staffed by former government officials, is backed by substantial government funding (approximately $21 billion, and nearly 19 billion in a projected second round),[154] and has used its resources to support numerous technology-related outbound investments in the United States.[155]

2. Chinese Investment Vehicles Used to Acquire and Transfer U.S. Technologies and IP

Chinese State actors implement China's outbound FDI program through investment vehicles that include mergers and acquisitions, seed and venture capital financing, and greenfield investing, particularly in strategically targeted high-technology industries.

a. Mergers & Acquisitions

The most direct way to acquire U.S. or other foreign IP or technology is for a Chinese entity to buy or otherwise gain a controlling stake in U.S. companies. As the U.S.-China Economic and Security Review Commission notes, this is the most common form of investment in the United States:

> *In 2016, acquisitions accounted for 96 percent of Chinese investment in the United States by value. Meanwhile, capital-intensive greenfield investments—including manufacturing plants, real estate developments, and R&D-intensive projects—accounted for only 4 percent of all U.S.-bound Chinese investments in 2016. This trend continued in the first half of 2017, with acquisitions comprising 97.6 percent of the total value of Chinese investment in the United States.* [156]

Chinese industrial policy documents reference the use of overseas mergers and acquisitions as part of its "Going Out" strategy to acquire "key technology" in sectors ranging from "next-generation" artificial intelligence[157] and biotechnology[158] to telecommunications and Internet enterprises.[159]

b. Greenfield Investments & Seed and Venture Funding

China's participation in greenfield investments and U.S. seed and venture funding deals that finance early-stage technology companies and startup firms is a relatively new phenomenon. On greenfield investing, the DIUx Pentagon Report notes that: "In the past 10 years, China's investments in U.S. technology firms were limited to joint ventures or acquisitions, but now there are an increasing number of greenfield investments in venture-backed startups (both as limited partners of U.S. venture firms and through Chinese venture firms) as well as investments through Chinese private equity firms."[160]

The China-based venture capital fund Sinovation illustrates the broader use of venture funding to acquire leading edge American technologies. Since its founding in 2009, Sinovation has accumulated $1.2 billion in total capital and "has invested in almost 300 startups – including 25 in artificial intelligence."[161] The DIUx Pentagon Report warns of the risks associated with Chinese venture funding:

> *The technologies China is investing in are the same ones that we expect will be foundational to future innovation in the U.S.: artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics and block chain technology. Moreover, these are some of the same technologies of interest to the US Defense Department to build on the technological superiority of the U.S. military today.*[162]

The DIUx Pentagon Report further notes that: "Chinese participation in venture-backed startups is at a record level of 7-10% of all venture deals done and has grown quite rapidly in the past five years."[163] Venture funding allows China to accomplish its objective of gaining access to leading companies in targeted technology sectors while drawing less scrutiny from governments wary of technology transfer risks.

III. Conclusion

This report has documented the two major strategies and various acts, policies, and practices Chinese industrial policy uses in seeking to acquire the intellectual property and technologies of the world and to capture the emerging high-technology industries that will drive future economic growth. The vectors of China's economic aggression in the technology and IP spaces that have been documented in this report are summarized in Table One on the next page.

Given the size of China's economy, the demonstrable extent of its market-distorting policies, and China's stated intent to dominate the industries of the future, China's acts, policies, and practices of economic aggression now targeting the technologies and IP of the world threaten not only the U.S. economy but also the global innovation system as a whole.

The Appendix to this report provides a compendium of the more than 50 acts, policies, and practices China uses to implement the six categories of Chinese economic aggression presented in the introduction to this report.

SEE TABLE ONE NEXT PAGE

Table One: Vectors of China's Economic Aggression in the Technology and IP Space

1. Physical Theft and Cyber-Enabled Theft of Technologies and IP
    - Physical Theft of Technologies and IP Through Economic Espionage
    - Cyber-Enabled Espionage and Theft
    - Evasion of U.S. Export Control Laws
    - Counterfeiting and Piracy
    - Reverse Engineering
2. Coercive and Intrusive Regulatory Gambits
    - Foreign Ownership Restrictions
    - Adverse Administrative Approvals and Licensing Requirements
    - Discriminatory Patent and Other IP Rights Restrictions
    - Security Reviews Force Technology and IP Transfers
    - Secure and Controllable Technology Standards
    - Data Localization Mandates
    - Burdensome and Intrusive Testing
    - Discriminatory Catalogues and Lists
    - Government Procurement Restrictions
    - Indigenous Technology Standards That Deviate From International Norms
    - Forced Research and Development
    - Antimonopoly Law Extortion
    - Expert Review Panels Force Disclosure of Proprietary Information
    - Chinese Communist Party Co-opts Corporate Governance
    - Placement of Chinese Employees with Foreign Joint Ventures
3. Economic Coercion
    - Export Restraints Restrict Access to Raw Materials
    - Monopsony Purchasing Power
4. Information Harvesting
    - Open Source Collection of Science and Technology Information
    - Chinese Nationals in U.S. as Non-Traditional Information Collectors
    - Recruitment of Science, Technology, Business, and Finance Talent
5. State-Sponsored, Technology-Seeking Investment
    - Chinese State Actors Involved in Technology-Seeking FDI
    - Chinese Investment Vehicles Used to Acquire and Transfer U.S. Technologies and IP
        - Mergers and Acquisitions
        - Greenfield Investments
        - Seed and Venture Funding

ENDNOTES

[1] "2017 Annual Report," US-China Economic and Security Commission, November 15, 2017, p. 24.
https://www.uscc.gov/sites/default/files/annual_reports/2017_Annual_Report_to_Congress.pdf

[2] The World Bank, "The World Bank in China," March 28, 2017.
http://www.worldbank.org/en/country/china/overview
According to the International Monetary Fund, China is the world's largest economy based on purchasing power parity, share of the world. IMF DataMapper. October, 2017.
https://www.imf.org/external/datamapper/PPPSH@WEO/OEMDC/ADVEC/WEOWORLD

[3] See United States Trade Representative, 2017 Report to Congress on China's WTO Compliance, January 2018.
https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf.
See also United States Trade Representative, "Section 301 Investigation of China's Acts, Practices, and Policies Related to Technology Transfer, Intellectual Property, and Innovation," March, 2018. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/march/section-301-report-chinas-acts

[4] The designation of China as a "strategic competitor" engaged in "economic aggression" was formalized in United States government policy with the December 2017 release of the White House National Security Strategy.
https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/

[5] Key documents range from the five-year plans that articulate Chinese goals and industrial policies and the landmark *2006 National Medium and Long Term Plan for Science and Technology*, which extends to 2020, to the more recent *Made in China 2025* and government reports on China's One-Belt, One-Road Initiative, a Chinese strategy to dominate much of the infrastructure, resources, and trading routes of the world. (See citations in endnotes that follow). See also the "The Belt and Road Initiative," National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce, People's Republic of China, March 28, 2015. And: "Made in China 2025," Gov.cn, Jan 8, 2018,
http://english.gov.cn/2016special/madeinchina2025/

[6] Actors include State-Owned Enterprises like China Mobile and Sinopec; sovereign wealth funds like China Investment Corp (CIC) and SAFE Investment Company; bureaucrats that control industrial policy agencies like the Ministry of Industry and Information Technology; Chinese military personnel in the People's Liberation Army that execute China's state-sponsored cyber espionage, and Chinese nationals that travel the world as students, scientists, engineers, venture capitalists, and business people.

[7] Some of those, on which this document has relied, include reports on China's trade practices produced by Chambers of Commerce in America and Europe; thousands of pages of hearings and reports generated by the bi-partisan U.S.-China Economic and Security Commission; documentation of China's behaviors at agencies like the Department of Commerce, the Department of Justice, and the U.S. Trade Representative; and the threat assessments of cyber security firms like Mandiant. Each of these sources will be referenced in the course of this report.

[8] For a review of Chinese protectionism, see, for example, *Chapter 1: U.S.-China Economic and Trade Relations* p. 35-140 of "2017 Annual Report," US-China Economic and Security Commission, November 15, 2017, https://www.uscc.gov/Annual_Reports/2017-annual-report.
See also "American Business in China," AmCham China, 2017. https://www.amchamchina.org/policy-advocacy/white-paper/

[9] As the U.S.-China Economic and Security Review Commission notes in its 2012 Report regarding China's use of national champions in its industrial policy: "China's indigenous innovation policies and additional attention to certain strategic sectors identified in its 12th Five-Year Plan ensure that it will continue to provide support to national champions. For the foreseeable future, such companies will continue to be favored over foreign firms for government and state-owned enterprise procurement contracts and will continue to benefit from a range of subsidies, tax breaks, special development funds, increased credit support, and other assistance not enjoyed by their foreign competitors. These advantages continue to make Chinese national champions formidable competitors in China and in other markets globally, undermining U.S. industry innovation and success." p. 5. The report also notes: "The 12th Five-Year Plan (2011–2015) also created ''strategic emerging industries'' such as green energy, biotechnology and nanotechnology, which will be advanced by ''national champions'' selected from among state-controlled companies and nurtured with government subsidies and preferences." p. 57. https://www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf

[10] It is unclear whether China deliberately uses overcapacity to gain control of industries. A competing view is that such overcapacity is the result of factors within China beyond the central government's control, e.g., the entrepreneurial efforts of local and provincial governments to stimulate growth in their jurisdictions.

[11] China controls over 95 percent of the world's rare earth minerals; see "Rare Earths: Battling China's Monopoly After Molycorp's demise," *Mining.com,* September 10, 2016. http://www.mining.com/rare-earths-battling-chinas-monopoly-after-molycorps-debacle/

[12] China's mercantilist approach to securing global resources is documented, for example, in Peter Navarro and Greg Autry, *Death By China*, Pearson FT Press, May 2011, Chapter 7. See also "2017 Annual Report," U.S.-China Economic and Security Commission, November 15, 2017. https://www.uscc.gov/Annual_Reports/2017-annual-report

[13] For additional documentation of China's efforts to dominate global manufacturing, see Peter Navarro and Greg Autry, *Death By China*, Pearson FT Press, May 2011.

[14] European Chamber of Commerce in China, "China Manufacturing 2025," February, 2017. p. 2. http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf

[15] According to the European Chamber of Commerce in China, "China Manufacturing 2025," February, 2017, one of the reasons China is turning its attention to capturing industries of the future is that today's manufacturing industries tend to be low value-added, energy-intensive, and highly polluting. p. 3.
http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf
Other reasons cited by the European Chamber include the need to raise income levels and reduce China's dependence on foreign technologies. This is a key goal of President Xi Jinping. See "Xi Jinping: Speech at the 17th Conference of the Chinese Academy of Sciences and 12th Conference

of the Chinese Academy of Engineering," Chinese Communist Party News, June 9, 2014. http://cpc.people.com.cn/n/2014/0610/c64094-25125594.html

[16] By construction, this report is not intended as a comprehensive, whole-of-government assessment of Chinese industrial policy. Nor does it assess every threat vector.

[17] *Notice on Issuing the National Medium- and Long-Term Science and Technology Development Plan Outline (2006-2020)*, State Council, Guo Fa, 2005 No. 44, issued Dec. 26, 2005).

[18] As noted by the U.S. International Trade Commission in its November 2010 Report: The goal of promoting Chinese intellectual property was reinforced in China's 2008 National Intellectual Property Strategy (NIPS).
https://www.usitc.gov/publications/332/pub4199.pdf

[19] For an overview of Chinese industrial espionage, see William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, (London: Routledge, 2013), 219-220.

[20] Cited in U.S. Trade Representative, *2013 Special 301 Report,* p. 13. https://ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf For main source, see Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October, 2011.
http://www.ncix.gov/publications/reports/fecie_all/%20Foreign_Economic_Collection_2011.pdf.

[21] Testimony by Ms. Jen Weedon on June 15, 2015 before the U.S.-China Economic and Security Review Commission, p. 3. https://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf

[22] U.S.-China Economic and Security Review Commission 2016 Annual Report to Congress, p. 3. https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf

[23] DIUx was formed by the Department of Defense in April 2015. A DoD website describes DIUx as a "fast-moving government entity that provides non-dilutive capital to companies to solve national defense problems." https://www.diux.mil/ The DIUx Pentagon Report was commissioned to assess the impacts of "China's participation in venture deals financing early-stage technology companies." p. 1. It was officially released in March 2018. https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf

[24] Brown, Michael, and Singh, Pavneet, "China's Technology Transfer Strategy," Defense Innovation Unit Experimental (DIUX), January, 2018. p. 15. (Hereinafter DIUx Pentagon Report) https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf

[25] "Revealing CCP's Special Politics: Guoan Yuli Aliens," *NTDTV.com,* June 6, 2015. http://www.ntdtv.com/xtr/gb/2015/06/02/a1200737.html

[26] Kania, Elsa, "China's Strategic Support Force: A Force for Innovation?" *The Diplomat,* February 18, 2017.
https://thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/

[27] "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage," Office of the National Counterintelligence Executive, October 2011. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-055.pdf, p. i.

[28] According to the testimony of Jeffrey Johnson before the U.S.-China Economic and Security Review Commission, cyber-economic campaigns "consist of state-sponsored and supported criminal cartels focused on leveraging cyber-enabled espionage and sabotage to execute industry-wide fraud, market manipulation and anti-trust schemes designed to accelerate

China's entry and domination of each key global industry." Hearing on "Chinese Investment in the United States." January 26, 2017. Hearing on "Chinese Investment in the United States." January 26, 2017.
https://www.uscc.gov/sites/default/files/Johnson_USCC%20Hearing%20Testimony012617.pdf

[29] According to the IP Commission, the cost of trade secret theft alone "is between 1% and 3% of GDP, meaning that the cost to the $18 trillion U.S. economy is between $180 billion and $540 billion," and China "remains the world's principal IP infringer." "The Theft of American Intellectual Property," IP Commission, February 2017, p. 2.
http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

[30] USTR Section 301 Investigation, p. 153.

[31] Verizon, "2013 Data Breach Investigations Report," p. 21.
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[32] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 19, 2013.
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[33] U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014.
https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[34] White House Fact Sheet, "President Xi Jinping's State Visit to the United States, September 25, 2015.
https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[35] U.S.-China Economic and Security Review Commission 2016 Annual Report to Congress, pp. 56-57.
https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf

[36] The Arms Export Control Act of 1976, 22 U.S.C. 2778.
https://www.pmddtc.state.gov/regulations_laws/aeca.html

[37] The AECA governs the export of defense articles and services, and the International Traffic in Arms Regulations (ITAR) is the implementation arm of AECA. The International Economic Emergency Powers Act (IEEPA), Title II of Public Law 95–223, 91 Statute 1626, enacted October 28, 1977, governs the export of military and dual use items through the Export Administration Regulations (EAR). The Export Administration Act (EAA) of 1979 (P.L. 96-72) was put in place to provide legal authority to the President to control U.S. exports for reasons of national security, foreign policy, or short supply; this authority was continued by executive and legal authority under IEEPA when the EAA expired in 1994. For IEEPA, see:
https://www.gpo.gov/fdsys/pkg/STATUTE-91/pdf/STATUTE-91-Pg1625.pdf

[38] "A Resource on Strategic Trade Management and Export Controls," U.S. Department of State,
https://www.state.gov/strategictrade/overview/

[39] Stutzman, Rene, "Orlando Smuggler Sentenced to 21 Months in Federal Prison," *Orlando Sentinel,* September 26, 2016. http://www.orlandosentinel.com/news/breaking-news/os-chinese-submarine-parts-smuggler-sentence-20160926-story.html

[40] U.S. Department of Justice, Summary Of Major U.S. Export Enforcement, Economic Espionage, Trade Secret And Embargo-Related Criminal Cases (January 2010 to the present: updated June 27, 2016)

https://www.pmddtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf

[41] According to the European Commission: "A counterfeit good is an unauthorised imitation of a branded good; and "pirated copyright goods shall mean any goods which are copies made without the consent of the right holder or person duly authorised by the right holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation." http://europa.eu/rapid/press-release_MEMO-10-272_en.htm

[42] 2017 Situation Report on Counterfeiting and Piracy in the European Union. p. 7. https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union

[43] "The Theft of American Intellectual Property," IP Commission Report Update, February 2017 p. 2. http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

[44] *Notice on Issuing the National Medium- and Long-Term Science and Technology Development Plan Outline (2006-2020)*, State Council, Guo Fa, 2005 No. 44, issued Dec. 26, 2005).

[45] European Chamber, "China Manufacturing 2025: Putting Industrial Policy ahead of Market Forces," p. 15. http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf

[46] US-China Business Council, "2017 Member Survey." p. 9. https://www.uschina.org/sites/default/files/2017_uscbc_member_survey.pdf

[47] As noted by the U.S. Department of State: "China maintains a more restrictive foreign investment regime than its major trading partners, including the United State … broad sectors of the economy remain closed to foreign investors." https://www.state.gov/e/eb/rls/othr/ics/2015/241518.htm

According to the U.S. Chamber of Commerce: "China has the most restrictive investment regime among G20 countries." U.S. Chamber of Commerce, "Made in China 2025: Global Ambitions Built on Local Protections," March 16, 2017. p. 8. (Hereinafter U.S. Chamber Made in China 2025 Report) https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[48] For example, China requires all foreign electronic vehicle (EV) companies wishing to manufacture automobiles in China to form joint ventures with Chinese companies with minority stakes. The foreign company must transfer EV technology to Chinese enterprises as they are building up their Chinese brands. In 2009, the Chinese Ministry of Industry and Information Technology (MIIT) hastened the pace of this forced technology transfer by requiring that one of the three key technologies essential to EVs (battery system, driving system, and electronic control system) have to be controlled by the Chinese company in joint ventures. https://www.uscc.gov/sites/default/files/Research/Planning%20for%20Innovation-Understanding%20China%27s%20Plans%20for%20Tech%20Energy%20Industrial%20and%20Defense%20Development072816.pdf

In January, 2017, MIIT issued updated regulations that "require NEV [New Energy Vehicle] manufacturers to master the development and manufacturing technology for the complete NEV, not just one of three core technologies." https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[49] "2017 Special 301 Report," *Office of the United States Trade Representative*, 2017. In placing China at the top of its Priority Watch List, the report notes that China "imposes requirements that US firms develop their IP in China or transfer their IP to Chinese entities as a condition to accessing the Chinese market." p. 1. https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF

[50] USTR Section 301 Investigation, p. 19

[51] As the U.S. Trade Representative notes, in referencing the written submission of the Information Technology and Innovation Foundation in the course of the USTR's Section 301 Investigation of China: "Chinese officials are careful not to put such requirements in writing, often resorting to oral communications and informal 'administrative guidance' to pressure foreign firms to transfer technology." USTR Section 301 Investigation, p. 19.

[52] Bradsher, Keith, and Mozar, Paul "As Washington Tries to Protect Tech, China Could Fight Back," *The New York Times,* August 2, 2017.
https://www.nytimes.com/2017/08/02/business/china-trade-trump-technology.html

[53] USTR Section 301 Investigation, p. 19.

[54] See, for example, China's draft Administrative Measures for the Formulation and Revision of National Standards Involving Patents released in December, 2012. According to the U.S.-China Business Council, this regulation "force[s] foreign companies to accept royalty rates lower than their ordinary worth." Specifically, Article 9 of the draft measures would require patent holders to license technology at a reasonable and nondiscriminatory rate that is "significantly lower than the normal licensing fee." U.S.-China Business Council, "The US-China Business Council Comments on Provisional Administrative Measures for the Formulation and Revision of National Standards Involving Patents (Draft)," Undated.
https://www.uschina.org/sites/default/files/patents_standards_comments_eng.pdf
Notes the *China Business Review* on such discriminatory royalty rights restrictions: "At least three features of China's royalties system appear to restrict royalty rates. First, China's tax authorities may limit the rates .... Second, late last year the standardization administration of China released draft Administrative Measures for the Formulation and Revision of National Standards Involving Patents, which may force foreign companies to accept royalty rates lower than their ordinary commercial worth. Specifically, Article 9 of the draft measures would require patent holders to license technology at a reasonable and nondiscriminatory rate that is 'significantly lower than the normal licensing fee'.... Third, in some cases, domestic companies may accept royalty arrangements only if the royalties are below standard market rates. This is driven, in part, by the belief among some Chinese companies that foreign industries are 'extracting' huge, seemingly disproportionate profits by their royalty demands." Moga, Thomas, "Tech Transfer Turning Point," September 1, 2010. *China Business Review. https://www.chinabusinessreview.com/tech-transfer-turning-point/*

[55] USTR Section 301 Investigation, p. 49.

[56] *Ibid.*

[57] USTR Section 301 Investigation, p. 54.

[58] *Ibid.*

[59] For a history, see, for example, Segal, Adam, "China, Encryption Policy, and International Influence," *Hoover Institution Series Paper No. 1610.* As Segal notes: "Encryption regulations have also been deployed as part of a larger effort to use standards policy to bolster the competitiveness of Chinese technology firms." November 28, 2016.
https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf

[60] *Cybersecurity Law of People's Republic of China*, National People's Congress of the People's Republic of China, 7th November, 2016. http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

[61] European Chamber, "China Manufacturing 2025: Putting Industrial Policy ahead of Market Forces," p. 24. http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf
[62] USTR Section 301 Investigation, p. 43.
[63] U.S. Chamber Made in China 2025 Report, p. 31. China has taken an expansive view of the application of this standard. At risk are sectors that include aviation, big data, banking, finance, cyber products, internet-related activities, industrial manufacturing, medical treatment and devices, and telecommunications.
[64] *Ibid*, p. 30.
[65] *Ibid*, p. 32.
[66] See, for example, China's recent comprehensive restrictions on all cross-border flow of data in China's June 2017 Cybersecurity Law. It established sweeping security reviews for products and services; imposes restrictions on the cross-border flow of data; requires data localization; and authorizes the development of national security standards that exceed the burden and scope of international standards. U.S. Chamber, *Submission, Section 301 Hearing 33-34* (Oct. 3, 2017). http://www.theglobalepicenter.com/wp-content/uploads/2013/01/USCC-2017-Special-301-Submission-Final.pdf
[67] U.S. Chamber, *Submission*, *Section 301 Hearing* 33-34 (Oct. 3, 2017). http://www.theglobalipcenter.com/wp-content/uploads/2013/01/USCC-2017-Special-301-Submission-Final.pdf.
[68] InCompliance, "New CCC Regulations in China," January 30, 2015. https://incompliancemag.com/article/new-ccc-regulations-in-china/
[69] TUV Rheinland of North America, "China Compulsory Certification," Undated. http://wll.com/us/wp-content/uploads/China%20Compulsory%20Certification%209.04.pdf
[70] Practical Law, "MIIT Releases 2015 Telecoms Catalogue," January 22, 2016. https://content.next.westlaw.com/Document/I41aed0b7c08b11e598dc8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1
[71] U.S. Chamber Made in China 2025 Report, p. 28.
[72] *Ibid.*
[73] European Chamber Report, p. 16.
[74] Josh Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, *Made in China 2025: The Making of a High-Tech Superpower and Consequences For Industrial Countries, Mercator Institute for China Studies, December 2016.* p. 56. https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf
[75] U.S. Chamber Made in China 2025 Report, p. 35.
[76] "American Business in China," AmCham China, 2017, p. 110. https://www.amchamchina.org/policy-advocacy/white-paper/
[77] China plans to "set or revise over 500 standards in smart manufacturing." U.S. Chamber Made in China 2025 Report. p. 34.
[78] European Chamber, p. 16.
[79] U.S. Chamber Made in China 2025 Report, p. 35.
[80] USTR Section 301 Investigation, p. 39,
[81] Official Chinese government documents identify "establishing foreign R&D centers" as an important method of acquiring foreign technology. USTR Section 301 Investigation, p. 12.
[82] USTR Section 301 Investigation, p. 32. See also U.S. CHAMBER, Submission, Section 301 Hearing 16 (Oct. 3, 2017).

[83] Ministry of Industry and Information Technology, Formal Announcement of Guidelines for the Development and Promotion of the Integrated Circuit Industry § 4(8), June 24, 2014.
[84] As the USTR Section 301 Investigation notes: "U.S. companies acquired by AVIC [Aviation Industry Corporation of China] now provide ongoing R&D and fill critical nodes in China's GA aircraft and piston engine manufacturing industry." USTR Section 301 Investigation, p. 109. See also USTR Section 301 Investigation, pp. 180-181.
[85] In a letter to Secretary of State John Kerry and Treasury Secretary Jacob Lew, the U.S. Chamber of Commerce wrote: "It has become increasingly clear that the Chinese government has seized on using the AML to promote Chinese producer welfare and to advance industrial policies that nurture domestic enterprises, rather than the internationally accepted norm of using competition law to protect consumer welfare and competition." See also Miller, Mathew. "China's Latest Anti-Trust Probes Revive Protectionist Concerns." *Reuters.* August 7, 2014. https://www.reuters.com/article/us-china-antitrust/chinas-latest-anti-trust-probes-revive-protectionism-concerns-idUSKBN0G70VA20140807
[86] Randewich, Noel and Miller, Matthew, "Qualcomm to Pay $975 Million to Resolve China Antitrust Dispute, *Business New,* February 9, 2015. https://www.reuters.com/article/us-china-qualcomm/qualcomm-to-pay-975-million-to-resolve-china-antitrust-dispute-idUSKBN0LD2EL20150209
[87] For example, an Expert Review Panel may "assess the safety, environmental impact, and energy conservation of a proposed investment." USTR Section 301 Investigation, p. 42.
[88] USTR Section 301 Investigation, p. 42. As an example offered by the U.S. Chamber of Commerce: "One company that submitted its safety assessment to an approval agency was required to provide specific temperature and pressure range information for its process equipment...that would make it easier for a competitor to learn about a production process the company considered to be a trade secret." In USTR Section 301 Investigation, p. 42.
[89] "Company Law of the People's Republic of China (Revised in 2013): Article 19," Standing Committee of the National People's Congress, December 28, 2013. www.fdi.gov.cn/1800000121_39_4814_0_7.html
[90] Notes the *New York Times*, in a November 2017 speech, "Mr. Xi called on officials to strengthen the party in 'government, the military, society and schools, north, south, east and west.' The message was quick to reach party members lower down in the ranks. Soon after Mr. Xi's speech, party officials in the central province of Hunan issued a notice to members instructing them to write the party into legal documents for private and state-owned companies alike. The document was accidentally made public when a local state-owned newspaper published it, but it was quickly taken down." Stevenson, Alexandra. "China's Communists Rewrite the Rules for Foreign Business." *New York Times,* April 13, 2018. https://www.nytimes.com/2018/04/13/business/china-communist-party-foreign-businesses.html
[91] The extension of this strategy to joint venture partners represents an escalation of the policy. Open source reporting indicates that foreign companies have had decisions overruled by the Chinese Communist Party, e.g., a joint venture by Cummins of Indiana was prohibited from hiring a manager. Stevenson, Alexandra. "China's Communists Rewrite the Rules for Foreign Business." *New York Times,* April 13, 2018. https://www.nytimes.com/2018/04/13/business/china-communist-party-foreign-businesses.html
[92] As an example noted in open source reporting: "the amended article of association of Beijing-based engineering contractor China Machinery Engineering Corp" specifies that "when making decisions on significant matters, the Board shall seek advice from the Party committee of the

Company." Hunter, Gregor, and Russolillo, Steven. "Now Advising China's State Firms: The Communist Party." *Wall Street Journal,* August 17, 2017. https://www.wsj.com/articles/now-advising-chinas-state-firms-the-communist-party-1502703005

[93] Feng, Emily. "Chinese Tech Giants Like Baidu and Sina Set Up Communist Party Committees. October 11, 2017. http://www.afr.com/news/world/asia/chinese-tech-giants-like-baidu-and-sina-set-up-communist-party-committees-20171011-gyyh5u

[94] Jing, Meng, "China's First 'Deep Learning Lab' Intensifies Challenge to US in Artificial Intelligence Race," *South China Morning Post*, February 21, 2017. http://www.scmp.com/tech/china-tech/article/2072692/chinas-first-deep-learning-lab-intensifies-challenge-us-artificial

[95] Martina, Michael, "Exclusive: In China, The Party's Push for Influence Inside Foreign Firms Stirs Fears, Reuters, Aug. 24, 2017. https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU

[96] USTR Section 301 Investigation, p. 28. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

[97] European Commission, "WTO Appellate Body Confirms: China's Export Restrictions on Rare Earths and Other Raw Materials Illegal," August 7, 2014. http://trade.ec.europa.eu/doclib/press/index.cfm?id=1050

[98] European Commission, "Critical Raw Materials," https://ec.europa.eu/growth/sectors/raw-materials/specific-interest/critical_en

[99] European Commission, "WTO Appellate Body Confirms: China's Export Restrictions on Rare Earths and Other Raw Materials Illegal," August 7, 2014. http://trade.ec.europa.eu/doclib/press/index.cfm?id=1050

[100] 2017 USTR Report to Congress on China's WTO Compliance. pp. 44-45. https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf

[101] As an example, the USTR notes: "China's treatment of coke, a key steel input, provided a clear example of the trade distortions engineered by China's export restraints. In 2008, China produced 336 million MT of coke, but it limited exports of coke to 12 million MT and additionally imposed 40 percent duties on coke exports. The effects of the export restraints on pricing were dramatic. In August 2008, the world price for coke reached $740." 2017 USTR Report to Congress on China's WTO Compliance. pp. 44-45. https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf

[102] For example, as the USTR Section 301 Investigation notes: "The fact that China's three largest airlines – Air China, China Eastern, and China Southern – are all state-owned and account for the vast majority of aircraft purchases provides the Chinese government with a significant degree of leverage over foreign aircraft makers." p. 33.

[103] DIUx Pentagon Report, pp. 19.

[104] *Ibid.*

[105] *Ibid.* The quotation within the quotation is attributed to Hannas, et. al, *China Industrial Espionage*, p. 22.

[106] As noted on its website, the Institute of Scientific and Technical Information of China as of 2010 had "collected 1.5 million domestic theses or dissertations, 220,000 overseas theses or dissertations, 100,000 conference proceedings in foreign languages, and 60,000 domestic conference proceedings. It has also collected 1.23 million copies of four major U.S. government

reports published since 1958, and more than 4,000 titles/year of foreign journals. It has possessed some 300,000 reference books published abroad, and opened up 18 electronic platforms for reference search, including Web of Knowledge, CA, NSI, NTIS, EI, INSPEC, among others. ISTIC has created 33 full text data bases, covering more than 7,500 titles of full-text digitized journals and 1,000 titles of proceedings, and made them available to the public access. Meanwhile, the Institute enjoys the collection of some 4,000 monographs or papers authored and donated by more than 1,000 academicians of the Chinese Academy of Sciences and the Chinese Academy of Engineering. Of the digital collections possessed by the Institute, the abstracts, published either at home or abroad, reached 45.23 million entries, with an annual addition up to 3.3 million entries. Chinese and foreign citations have risen to 82.86 million entries, with an annual addition of 15.5 million entries." http://www.istic.ac.cn/English/

[107] Huo Zhongwen and Wang Zongxiao, *Sources and Methods of Obtaining National Defense Science & Technology Intelligence*, Kexue Jishu Wenxuan Publishing Co., Beijing, 1991. https://fas.org/irp/world/china/docs/sources_chap7.html

[108] For this descriptor, see, for example, Roper, Carl, *Trade Secret Theft, Industrial Espionage, and the China Threat,* CRC Press, December 2013. https://www.taylorfrancis.com/books/9781439899397

[109] *Ibid*, see Chapter 2.

[110] Huo Zhongwen and Wang Zongxiao, Sources and Methods of Obtaining National Defense Science & Technology Intelligence, Kexue Jishu Wenxuan Publishing Co., Beijing, 1991. https://fas.org/irp/world/china/docs/sources.html

[111] DIUx Pentagon Report, p. 17.

[112] Mattis, Peter, "A Guide to Chinese Intelligence Operations," *War on the Rocks,* August 18, 2015. https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/

[113] The term "non-traditional collector" is commonly used in the Intelligence Community to differentiate between traditional collectors such as spies. For an example of its use in discussing the threats associated with "non-traditional collectors such as post-graduate and graduate students applying for positions in cleared U.S. industry," see Defense Security Service, Department of Defense, "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry." http://www.dss.mil/counterintel/regionalTrends/eastAsiaPacific.html?sub5

[114] DIUx Pentagon Report, p. 17-18.

[115] *Ibid*, p. 19.

[116] CNN Transcript, Intelligence Chiefs Take Questions From Senate Intelligence Committee," February 13, 2018. http://transcripts.cnn.com/TRANSCRIPTS/1802/13/cnr.04.html

[117] *Ibid.*

[118] U.S. House of Representatives, "Investigative Report on the U.S. National Security Issues Posed by Telecommunications Companies Huawei and ZTE, October 8, 2012. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

[119] U.S. House of Representatives, National Defense Authorization Act For Fiscal Year 2018, p. 1224. https://docs.house.gov/billsthisweek/20171113/HRPT-115-HR2810.pdf For an analysis, see Wiley Rein, "Update on NDAA FY18 Cyber Provisions," February 2018. "https://www.wileyrein.com/newsroom-newsletters-item-Update-on-NDAA-FY18-Cyber-Provisions.html

[120] "Huawei Puts $1M into a New AI Research Partnership with UC Berkeley," Ingrid Lunden, *Tech Crunch*, October 11, 2016,

https://techcrunch.com/2016/10/11/huawei-puts-1m-into-a-new-ai-research-partnership-with-uc-berkeley/

[121] "DIUx Pentagon Report, p. 20. See also Yuan, Li, "China Races to Tap Artificial Intelligence," *Wall Street Journal,* August 24, 2016. https://www.wsj.com/articles/china-gears-up-in-artificial-intelligence-race-1472054254

[122] Stephen Chen, "America's Hidden Role in Chinese Weapons Research," South China Morning Post," March 29, 2017 http://www.scmp.com/news/china/diplomacy-defence/article/2082738/americas-hidden-role-chinese-weapons-research

[123] Berger, Zach. "Hypersonic Missiles," Missile Defense Advocacy Alliance. March 2016. http://missiledefenseadvocacy.org/missile-threat-and-proliferation/future-ballistic-missile-technology/hypersonic-missiles/

[124] "China's Program For Recruiting Foreign Scientists Comes Under Scrutiny," *South China Morning Post,* November 3, 2014. http://www.scmp.com/news/china/article/1631317/chinas-programme-recruiting-foreign-scientists-comes-under-scrutiny

[125] "Xinhua, "Chinese Students Overseas Inspired by Patriotism of Late Geophysicist," *China Daily,* July 13, 2017. http://www.chinadaily.com.cn/china/2017-07/13/content_30101355.htm

[126] President Xi Jinping is quoted as saying, "You are warmly welcome if you return to China. If you stay abroad, we support you in serving the country in various ways." See http://usa.chinadaily.com.cn/epaper/2013-10/22/content_17050714.htm.

[127] Programs include the Chinese Academy of Sciences' Hundred Talents Plan, the High-level Visiting Scholar Plan Special Fund for Overseas Scholars to Return to China for Short Periods to Work and Lecture and the Young Overseas Scholars Cooperative Research Fund. See, for example, "China Launches 12 Programs to Attract Talent," *China Daily,* November 11, 2011. http://www.chinadaily.com.cn/china/2011-11/11/content_14081037.htm

[128] Jia, Hepeng. "China's Plan to Recruit Talented Researchers," January 17, 2019. https://www.nature.com/articles/d41586-018-00538-z

[129] "Returnees Finding Big Opportunities," Su Zhou, *China Daily,* February 25, 2017, http://www.chinadaily.com.cn/china/2017-02/25/content_28345785.htm

[130] *Ibid.*

[131] USTR Section 301 Investigation, p. 65.

[132] As the USTR Section 301 Investigation documents: "Investments that are 'encouraged' receive several forms of government support, including: (1) subsidies for fees incurred, and bank loans at government-subsidized interest rates; (2) policy bank loan support; (3) priority administrative approval; (4) priority support for the use of foreign exchange; (5) export tax rebates on exports of equipment and other materials relating to the overseas investment project; (6) priority access to services relating to overseas financing, investment consultation, risk evaluation, risk control, and investment insurance; and (7) coordinated support from several government departments with respect to information exchange, diplomatic protections, the travel of personnel abroad, and registration of import and export rights." p. 78.

[133] *Overseas Investment Industrial Guiding Policy,* July 5, 2006.

[134] Three of the world's ten largest sovereign wealth funds are from China and handle more than $1.5 trillion in assets. These three funds, according to the Sovereign Wealth Fund Institute, include: CIC (third-ranked, $813.8 billion in assets); SAFE Investment Company (seventh-ranked,

$441 billion in assets); and the National Social Security Fund ("NSSF") (tenth-ranked, $295 billion in assets). "Sovereign Wealth Fund Rankings – Largest Sovereign Wealth Funds Under Management," Sovereign Wealth Fund Institute. https://www.swfinstitute.org/sovereign-wealth-fund-rankings/

[135] State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015, staff translation.

[136] For an analysis of the protectionist and mercantilist implications of Made in China 2025, see, for example, Josh Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, *Made in China 2025: The Making of a High-Tech Superpower and Consequences For Industrial Countries, Mercator Institute for China Studies, December 2016.* https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf and U.S. Chamber Made In China 2025 Report. https://www.uschamber.com/report/made-china-2025-global-ambitions-built-local-protections-0

[137] "From China with Love: AI, Robotics, AR/VR Are Hot Areas For Chinese Investment In US," *CB Insights,* August 1, 2017. https://www.cbinsights.com/research/chinese-investment-us-tech-expert-research/

[138] Wee, Sui-Lee, "China's $800 Billion Sovereign Wealth Fund Seeks More U.S. Access," *New York Times,* July 11, 2017. https://www.nytimes.com/2017/07/11/business/china-investment-infrastructure.html.

[139] Schleifer, Theodore, "Chinese Investors Are Making Moves to Increase Their Spending in Silicon Valley," *Recode*, October 29, 2017. https://www.recode.net/2017/10/29/16568412/chinese-investors-silicon-valley-spending-china-investment-corporation

[140] "Xi Stresses CPC Leadership of State-Owned Enterprises," *Xinhua*, November 10, 2016. http://news.xinhuanet.com/english/2016-10/11/c_135746608.htm

[141] Scissors, Derek, "China's SOE Sector is Bigger Than Some Would Have Us Think," *American Enterprise Institute*, May 17, 2016. http://www.aei.org/publication/chinas-soe-sector-is-bigger-than-some-would-have-us-think/

[142] See, for example, Tiezzi, Shannon, "China Invests in the World," *The Diplomat,* June 24, 2015. https://thediplomat.com/2015/06/china-invests-in-the-world/

[143] See, for example, "The Rise of Private Firms in China Outbound Direct Investment," *China Chamber of Commerce in the Netherlands, https://www.dccchina.org/2016/09/the-rise-of-private-firms-in-china-outbound-direct-investment/*

[144] "2017 Annual Report," US-China Economic and Security Commission, November 15, 2017, p. 71. https://www.uscc.gov/sites/default/files/annual_reports/2017_Annual_Report_to_Congress.pdf

As noted by Reuters: the "legal argument concerns whether companies controlled by the Chinese government can be protected under the U.S. Foreign Sovereign Immunities Act (FSIA), which was passed by Congress in 1976, even when their U.S. subsidiaries are involved in commercial disputes." Miller, Matthew, and Michael Martina, "Chinese State Entities Argue They Have 'Sovereign Immunity' in U.S. Courts," *Reuters,* May 11, 2016. https://www.reuters.com/article/us-china-usa-companies-lawsuits/chinese-state-entities-argue-they-have-sovereign-immunity-in-u-s-courts-idUSKCN0Y2131.

For example, in March of 2016, a U.S. District Court Judge in Louisiana dismissed a defective drywall suit against the China New Building Materials Group on the grounds that it was "immune

under the Foreign Sovereign Immunities Act from claims in U.S. litigation since it is owned by a foreign government" and its alleged conduct was not subject to the commercial activity or tortious activity exceptions to immunity under the Act. China's global champion in the aviation sector, the Aviation Industry Corporation of China (AVIC), has sought similar protection in two other suits. This type of legal gambit conforms to an aggressive Chinese industrial policy that seeks to benefit from the rules of the free market when it is convenient but flaunts those rules when it is not. For more, see Sundar, Sindhu, "Chinese Co. Ducks MDL Claims Over Defective Drywall," *Law360*, March 15, 2016. https://www.law360.com/articles/771877/chinese-co-ducks-mdl-claims-over-defective-drywall

[145] "2017 Annual Report," U.S.-China Economic and Security Commission, November 15, 2017, p. 80.
https://www.uscc.gov/sites/default/files/annual_reports/2017_Annual_Report_to_Congress.pdf
For more on the role of SOEs in China's economy, see U.S.-China Economic and Security Review Commission, Chapter 1, Section 2, "State-Owned Enterprises, Overcapacity, and China's Market Economy Status," in 2016 Annual Report to Congress, November 2016, 92–103 https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf
and Walsh, Dustin, "Gateway '17 Looks to Connect Michigan Business to China," Crain's Detroit Business, June 18, 2017.
http://www.crainsdetroit.com/article/20170618/NEWS/170619891/gateway-17-looks-to-connect-michigan-business-to-china

[146] "2016 Annual Report," U.S.-China Economic and Security Commission, 2016, p. 102. https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf The report bases the information on State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015, Staff translation; U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, written testimony of Willy C. Shih, June 15, 2011; U.S.-China Economic and Security Review Commission, *Hearing on the Extent of the Government's Control of China's Economy, and Implications for the United States*, written testimony of George T. Haley, May 24–25, 2007; and U.S.-China Economic and Security Review Commission, Chapter 1, Section 1, ''The Relationship's Current Status and Significant Changes during 2007,'' in 2007 Annual Report to Congress, November 2007, 38–39.

[147] US-China Business Council, "2017 Member Survey." p. 3.
https://www.uschina.org/sites/default/files/2017_uscbc_member_survey.pdf

[148] *Ibid.*

[149] " Rising Tension: Assessing China's FDI Drop in Europe and North America," Baker McKenzie and Rhodium Group, April 2018, p.7. https://www.bakermckenzie.com/-/media/files/insight/publications/2018/04/rising_tension_china_fdi.pdf?la=en

[150] Sovereign Investor Institute's Sovereign Wealth Center, January 2018. http://www.sovereignwealthcenter.com/fund/6/china-investment-corporation.html#.Wq1yNujwb-g

[151] Wübbeke, Jost, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," Mercator Institute for China Studies, December 2016, p. 53. *https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf*

[152]"National Integrated Circuit Industry Development Outline," Chinese Ministry of Industry & Information Technology, June 24, 2014.
http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757021/c3758335/content.html
[153] State Council, *Guideline for the Development and Promotion of the Integrated Circuit Industry*, Section 4(2). https://members.wto.org/CRNAttachments/2014/SCMQ2/law47.pdf
[154] USTR Section 301 Investigation, p. 92; Wu, Kane; Zhu, Julie; and Cadell, Cate, "Exclusive: Chip Wars – China Closing In On Second $19 Billion Semiconductor Fund: Sources," *Reuters*, April 26, 2018. *https://www.reuters.com/article/us-china-trade-fund-exclusive/exclusive-chip-wars-china-closing-in-on-second-19-billion-semiconductor-fund-sources-idUSKBN1HX191*..
[155] Ye, Tianchun, "Guidelines to Promote National IC Industry Development," U.S. Information Technology Office.
https://www.semiconductors.org/clientuploads/China%20IC%20docs/B/YeTianchun%20Analysis%20(2).pdf
[156] "2017 Annual Report," U.S.-China Economic and Security Commission, November 15, 2017, p. 78.
https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf
See also written testimony of Timothy R. Heath before the U.S.-China Economic and Security Review Commission, Hearing on Hotspots along China's Maritime Periphery, April 13, 2017; https://www.uscc.gov/sites/default/files/transcripts/April%20Hearing%20Transcript.pdf;
China's State Council Information Office, The Diversified Employment of China's Armed Forces, April 16, 2013; http://www.nti.org/media/pdfs/China_Defense_White_Paper_2013.pdf; and Ryan Martinson, "The Militarization of China's Coast Guard," *The Diplomat*, November 21, 2014. https://thediplomat.com/2014/11/the-militarization-of-chinas-coast-guard/
[157] *State Council Notice on Issuing the Next-Generation of Artificial Intelligence Development Plan,* July 8, 2017. p. 24. https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf
[158] *MOST Notice on Issuing the "13th Five-year" Biotechnology Innovation Special Plan* Apr. 24, 2017.
[159] *International Cooperation Opinion* § 3(15). *Guiding Opinion on Promoting International Industrial Capacity and Equipment Manufacturing Cooperation* (*International Cooperation Opinion*), May 2015. http://www.gov.cn/zhengce/content/2015-05/16/content_9771.htm
[160] DIUx Pentagon Report, p. 9.
[161] *Ibid*, p. 8.
[162] *Ibid*, p. 1
[163] *Ibid*, p. 2

The Intercept_

THE FBI'S CHINA OBSESSION

The U.S. Government Secretly Spied on Chinese American Scientists, Upending Lives and Paving the Way for Decades of Discrimination

Harry Sheng, a former mechanical engineer for Sparton Corporation, photographed in the 1960s. Photo: Courtesy of Ling Woo Liu

Mara Hvistendahl

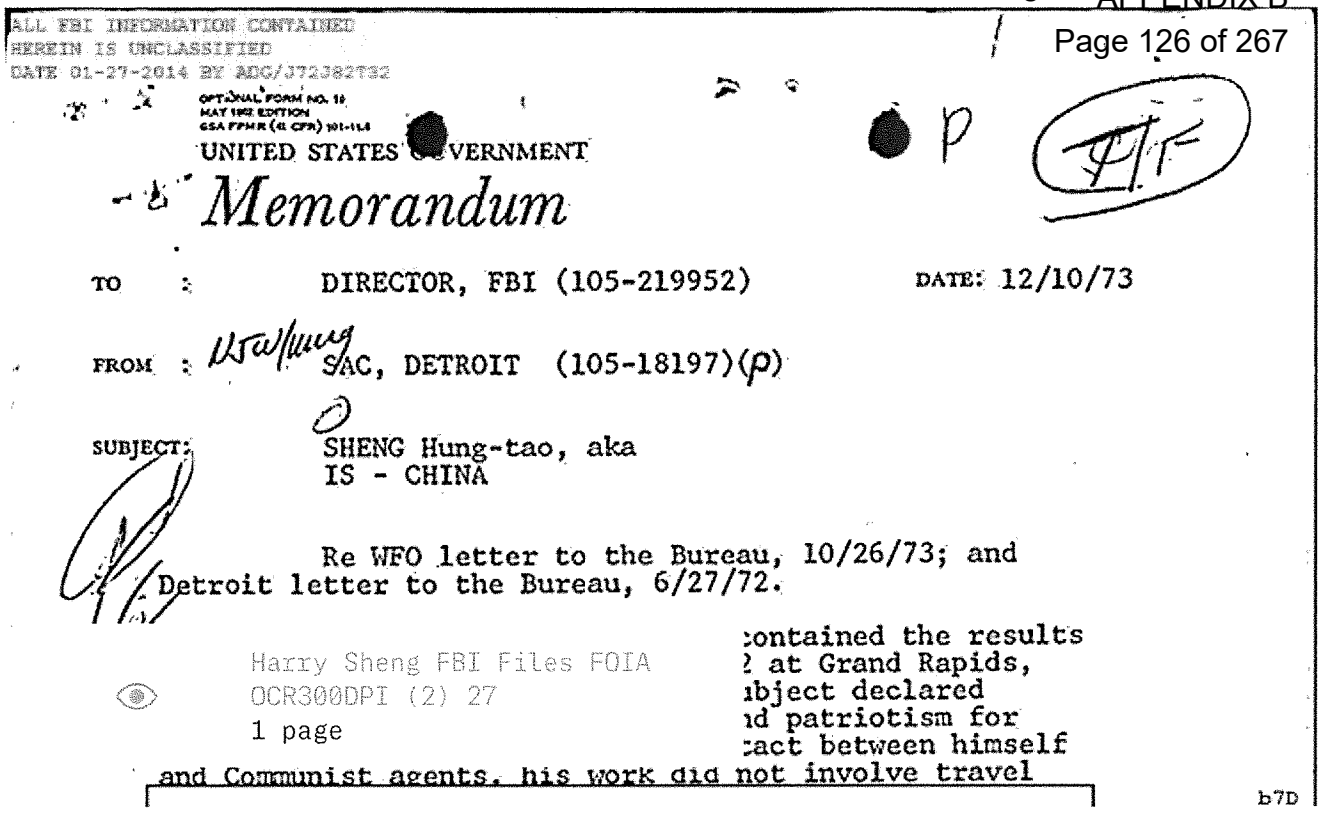
February 2 2020, 5:00 a.m.

In 1973, Harry Sheng was working as a mechanical engineer for Sparton Corporation, a defense contractor in Jackson, Michigan, when his mother got sick back in China. Sheng was among thousands of ethnic Chinese scientists then living in the United States, the early pioneers in what would become a sizable swath of the American research force. A native of Jiangsu province and a naturalized U.S. citizen, he had left home just before Mao Zedong came to power in 1949, and he hadn't seen his friends or relatives in China since. But now relations between the two countries were improving. In 1971, the U.S. pingpong team had toured the mainland, and the following year, President Richard Nixon had made the historic visit that restored contact between the countries'

leaders. Sheng had just started his job at Sparton, but he loved his mother dearly. He and his wife booked flights.

On Nixon's trip, the two sides had agreed to set up exchanges in science, which, like pingpong, was seen as a way to improve ties between the United States and China. Washington hoped that rapprochement with China would destabilize the Communist-led independence forces the U.S. military was fighting in Vietnam and increase America's leverage over the Soviet Union. For Chinese American scientists like Sheng, the thaw presented a simpler opportunity: a chance to return to their hometowns, eat their favorite foods, and hug the parents they had left behind decades earlier.

Sheng was a gentle man who collected coins in his spare time and never missed a church service. Before joining Sparton, he had worked for a decade for the defense contractor Lear Siegler, where he held a secret-level U.S. government security clearance. In 1972, he had been interviewed by an FBI agent in Grand Rapids, Michigan, for an undisclosed purpose. According to an FBI memo, Sheng "declared his anti-communist feelings, his love and patriotism for America" and "denied any contact between himself and Communist agents." But after Sheng and his wife returned from their 1973 visit to China, the U.S. government's scrutiny intensified. Agents from the FBI, the CIA, and the Department of Defense grilled him about everything he had done on his sightseeing tour, he later said. Sparton inexplicably transferred him to a drafting position – a move that he perceived as a demotion – and then, in 1975, laid him off. He subsequently received two offers from other defense firms, Raytheon and Hazeltine, only to have them suddenly rescinded, he said. He never held a permanent position in his field again.



ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-27-2014 BY ADC/J72J82T32

OPTIONAL FORM NO. 10
MAY 1962 EDITION
GSA FPMR (41 CFR) 101-11.6

UNITED STATES GOVERNMENT

Memorandum

TO : DIRECTOR, FBI (105-219952) DATE: 12/10/73

FROM : SAC, DETROIT (105-18197)(P)

SUBJECT: SHENG Hung-tao, aka
IS - CHINA

Re WFO letter to the Bureau, 10/26/73; and
Detroit letter to the Bureau, 6/27/72.

Harry Sheng FBI Files FOIA
OCR300DPI (2) 27
1 page

contained the results
at Grand Rapids,
ubject declared
id patriotism for
act between himself
and Communist agents, his work did not involve travel

b7D

Sheng was baffled. He had served in the marines for Chiang Kai-shek's Nationalist forces in the Chinese Civil War, against Mao's Liberation Army, and had no desire to live under Communist rule. The FBI sometimes investigated undocumented immigrants, including in San Francisco's Chinatown, but Sheng had married a white woman from Iowa, and he knew few other Chinese Americans in the Grand Rapids area. Sheng flew the American flag outside his house, and in his encounters with federal agents, he had seemingly done everything right. In a 1973 interview, an FBI agent asked him what he would do if the Communists pressured his relatives living in China. Sheng replied that he would immediately report the matter to the FBI.

He spent years searching for answers, but he never got the one that would have explained all the undue scrutiny: He was one of what appear to have been hundreds of people surveilled under a previously unreported FBI program that targeted ethnic Chinese scientists and students living in the United States. Titled "Chinese Communist Contacts with Scientists in the U.S." and listed under the umbrella "IS-CH," or Internal Security-China, the classified program dates to the late

1960s, when Chinese weapons development spurred intense anxiety within the U.S. government. It continued until at least 1978. The program's targets included several prominent scientists and scholars, most notably physicist Chang-Lin Tien, who later became chancellor of the University of California, Berkeley.

Under J. Edgar Hoover, the FBI pursued a slew of misguided counterintelligence investigations, hounding civil rights activists, feminist groups, and left-leaning scholars. The bureau's broader surveillance of scientists during the Cold War is well documented; among those targeted was theoretical physicist and Manhattan Project contributor Richard Feynman. The newly obtained documents show that alongside such efforts, the bureau singled out Chinese American scientists because of their ethnicity — and that it did so even after the Senate's Church Committee, formed in 1975, exposed some of the most egregious intelligence abuses of the era, many involving government surveillance of Americans on U.S. soil.

Program documents that I obtained through a Freedom of Information Act request, as well as the files of individual scientists who were surveilled, suggest a wide-ranging effort. They also show an early tendency within the U.S. national security establishment to assume that major scientific advances in China were the product of theft — a logic that would inform cases for decades to come. Zuoyue Wang, a historian at California State Polytechnic University in Pomona whose research focuses on U.S.-China scientific relations during the Cold War, said the documents show an inclination to assume that "American scientists with an immigrant background are the primary sources of illicit technological transfers," when in reality the story of technological advancement is much more complex.

The program's effects reverberate today, at a moment when combating economic espionage and scientific theft from China are among the FBI's

top priorities. Over the past decade, the Justice Department has brought dozens of cases involving ethnic Chinese scientists. It has also brought a number of cases against non-Chinese, most notably Charles Lieber, the chair of Harvard University's chemistry department, who was charged last week with making false statements in connection to grant money he received from the Chinese government. Critics allege that the broader campaign against intellectual property theft is often informed by the same thinking that drove the Chinese scientist program.

The FBI did not respond to a request for comment about the program or about ongoing complaints of bias against Chinese Americans both within and outside the bureau.

Join Our Newsletter
Original reporting. Fearless journalism. Delivered to you.
I'm in →

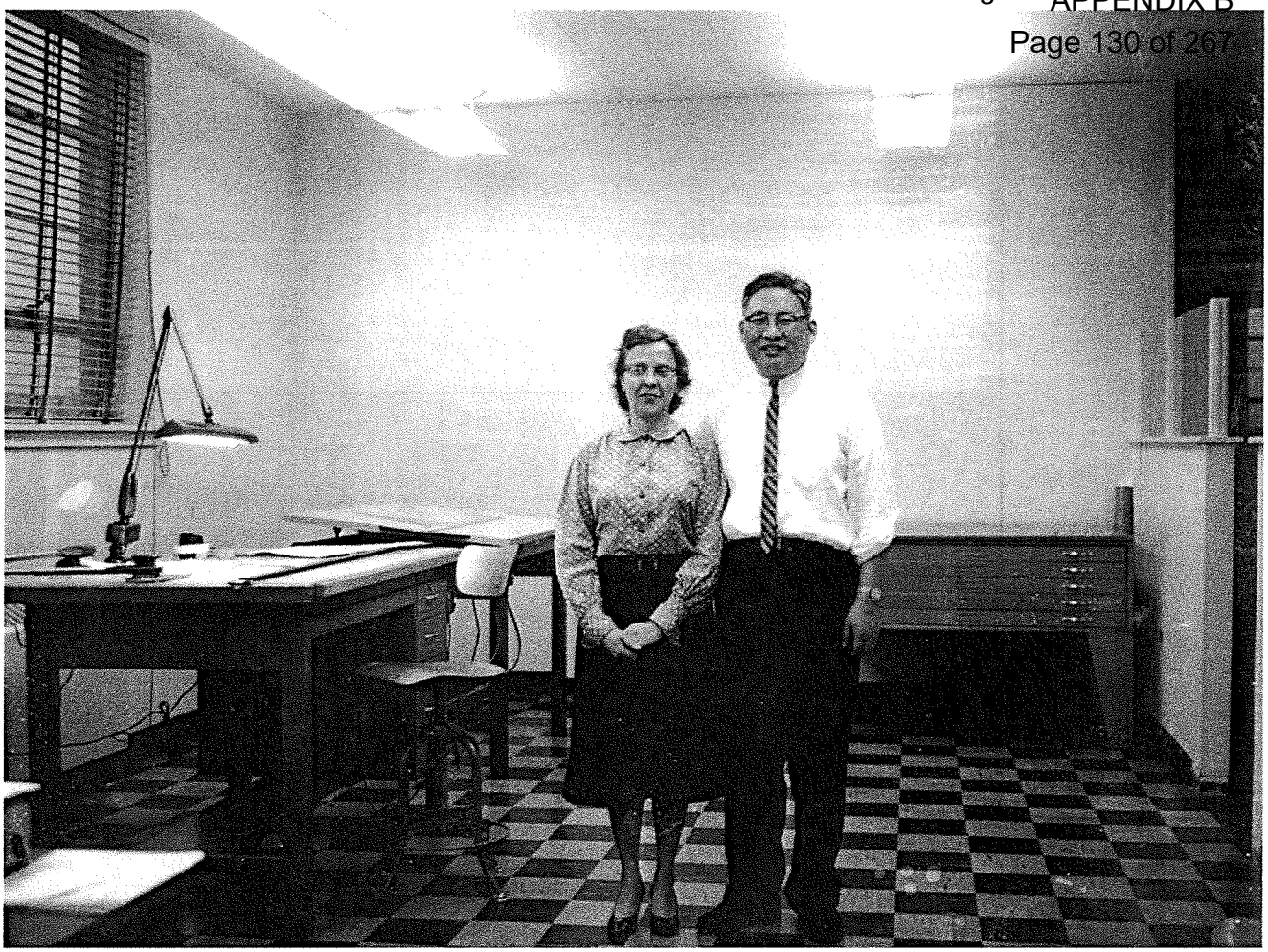
The focus on economic espionage began under the Obama administration, but as tensions with China have heightened under President Donald Trump, cases have proliferated. In 2018, the Justice Department's National Security Division launched an effort focused on intellectual property theft called the China Initiative. "No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China," FBI Director Christopher Wray said at the time. The FBI now says it has more than 1,000 active investigations into Chinese industrial espionage, spanning all 50 states.

Among the cases brought by federal prosecutors are clear-cut instances of technological theft, such as one against Chinese wind turbine firm Sinovel, which in 2018 was convicted of stealing the source code for operating wind turbines from Wisconsin-based American Superconductor. But not all the cases have panned out, and critics see bias in who is charged. In a 2019 analysis of 136 cases brought under the

Economic Espionage Act, Andrew Chongseh Kim, a visiting scholar at South Texas College of Law, found that 21 percent of defendants with Chinese names were ultimately not convicted of espionage or other major crimes, about twice the rate of defendants from other ethnic groups, meaning that they were either acquitted at trial or the most serious charges against them were downgraded or dropped.

One such botched investigation involved Xiaoxing Xi, an expert at Temple University in Philadelphia on superconducting thin films, which carry electricity without resistance at very low temperatures. In 2015, Xi was the interim chair of the university's physics department when he was charged with trying to transfer to China designs for a thin-film device called the pocket heater, which is made by Superconductor Technologies Inc. based in Austin, Texas. The charges against Xi were dropped after his lawyer submitted affidavits from other scientists – including the inventor of the pocket heater himself – making clear that there was little substance to the allegations.

The existence of a dedicated FBI program to surveil Chinese scientists, Xi told me, "sounds eerily like what is happening today."



Harry Sheng and his wife, Irene, in the 1960s. Photo: Courtesy of Ling Woo Liu

I first learned about the FBI's Chinese scientist program in a 2016 email from a Bay Area woman named Ling Woo Liu. I was part-way through writing a book, "The Scientist and the Spy: A True Story of China, the FBI, and Industrial Espionage," on an FBI investigation involving a Chinese-born scientist. That case was set in motion in 2011, when a researcher named Robert Mo was chased down by sheriff's deputies near a Monsanto contract field in Iowa. Mo had been driving a rental van while his colleague from a Beijing agriculture company surveyed the field for stray ears of corn. The FBI suspected the men of trying to reverse-engineer Monsanto and DuPont Pioneer hybrid corn seed.

Having spent eight years as a reporter in China, I was clear-eyed about the existence of industrial espionage, and my reporting suggested that Mo and his colleagues *were* trying to glean trade secrets from Monsanto

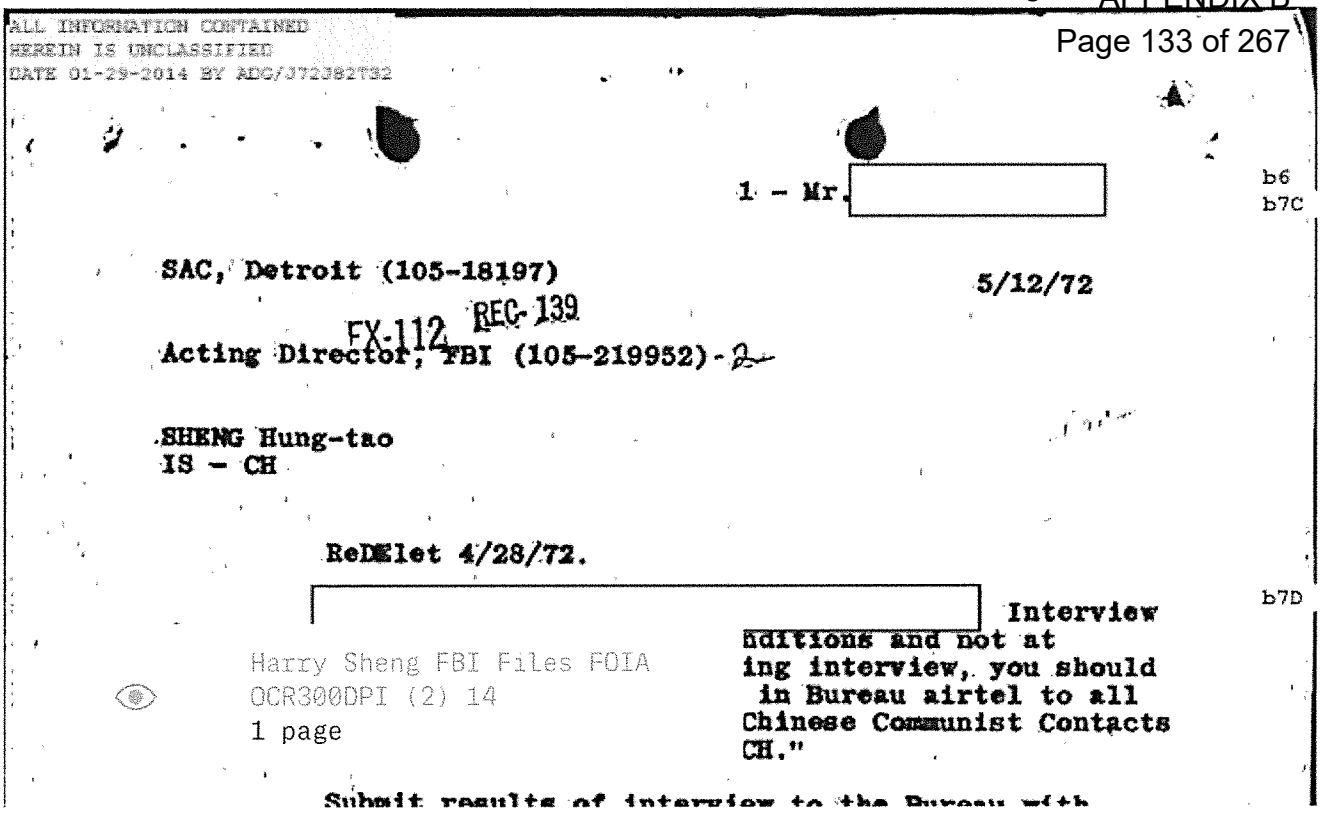
and DuPont Pioneer. But the FBI's reaction seemed disproportionate to the crime. The cornfield incident sparked a two-year investigation in which the bureau flew surveillance planes over the heartland, collected evidence using a Foreign Intelligence Surveillance Act warrant, and staged an elaborate airport bust involving microwave popcorn bags — all in the name of protecting the intellectual property of two giant corporations. The U.S. government spent untold amounts of money investigating and prosecuting Mo, ostensibly to safeguard American innovation. And yet, by the time I had finished the book, Monsanto had been acquired by the German conglomerate Bayer, meaning that it was no longer even American.

In the course of my reporting, I had talked with former prosecutors, intelligence analysts, and community organizers who detailed a longstanding history of bias against Chinese Americans within the bureau. So when Liu emailed me out of the blue to say that she had insight into that history, I was intrigued. We set up a phone call.

Harry Sheng had been a close friend of her parents, Liu told me. After several years of failing to find a steady job, his wife, Irene, began nannying for Liu and her sisters. The Shengs later followed the Liu family to California. The Shengs did not have children of their own, and they attended all of the girls' birthday parties, dance recitals, and soccer games. The sisters referred to them as "aunt" and "uncle" throughout their lives. Liu did not learn why Sheng had abruptly stopped working until decades later, after his death. Then, while sorting through his belongings, she and her sisters found a packet of papers containing years' worth of letters from Sheng to Michigan lawmakers, seeking answers about why he had been laid off.

Liu filed a FOIA request for Sheng's FBI file. When it arrived, she noticed the label "IS-CH" at the top of many documents. One 1972 letter in the file instructed agents in Detroit that when interviewing Sheng,

they should follow "instructions set forth in Bureau airtel to all offices, dated 9/22/71, captioned 'Chinese Communist Contacts with Scientists in the U.S.'"



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-29-2014 BY ADC/J72J82T32

1 - Mr. [redacted] b6 b7C

SAC, Detroit (105-18197) 5/12/72

FX-112 REC-139

Acting Director, FBI (105-219952) - 2

SHENG Hung-tao
IS - CH

ReDEtel 4/28/72.

[redacted] b7D Interview
additions and not at
ing interview, you should
in Bureau airtel to all
Chinese Communist Contacts
CH."

Submit results of interview to the Bureau with

Harry Sheng FBI Files FOIA
OCR300DPI (2) 14
1 page

"Have you heard of this program?" she asked me.

I hadn't, but I knew of other scientists who had been surveilled during that period. I filed a FOIA request for documents connected to the program. Two years later, after I had all but given up, the FBI sent me 105 pages of documents. They are marred by redactions, and the release only covers the year 1967, even though the program continued at least into the late 1970s. The FBI declined to release an additional 107 pages, on the basis that they were exempted from disclosure, would violate individuals' privacy, or reveal the agency's sources and methods. (At one point, the bureau redacted the name of a person described as "Communist Party Chairman" — Mao Zedong.) A Washington, D.C.-based law firm helped me appeal the bureau's decisions last spring. The request is still under review. But through additional FOIA requests, I obtained the files of other scientists surveilled under the program that helped round out the picture.

The Chinese scientist program has its origins in the 1950s Red Scare, when the FBI investigated Chinese-born rocket scientist Tsien Hsue-

Shen (later known as Qian Xuesen) for being a suspected member of the U.S. Communist Party. Tsien, whose story is detailed in Iris Chang's book "Thread of the Silkworm," was a talented researcher at the California Institute of Technology in Pasadena, where he worked on classified government projects and helped found Caltech's Jet Propulsion Laboratory. In 1950, the year after Mao rose to power in China, FBI agents questioned Tsien, and the U.S. military revoked his security clearance. Recent research suggests that for a while, Tsien was a party member, but that he showed little interest in aiding China. That changed when the FBI began scrutinizing his loyalty, making it impossible for him to do serious work in the United States.

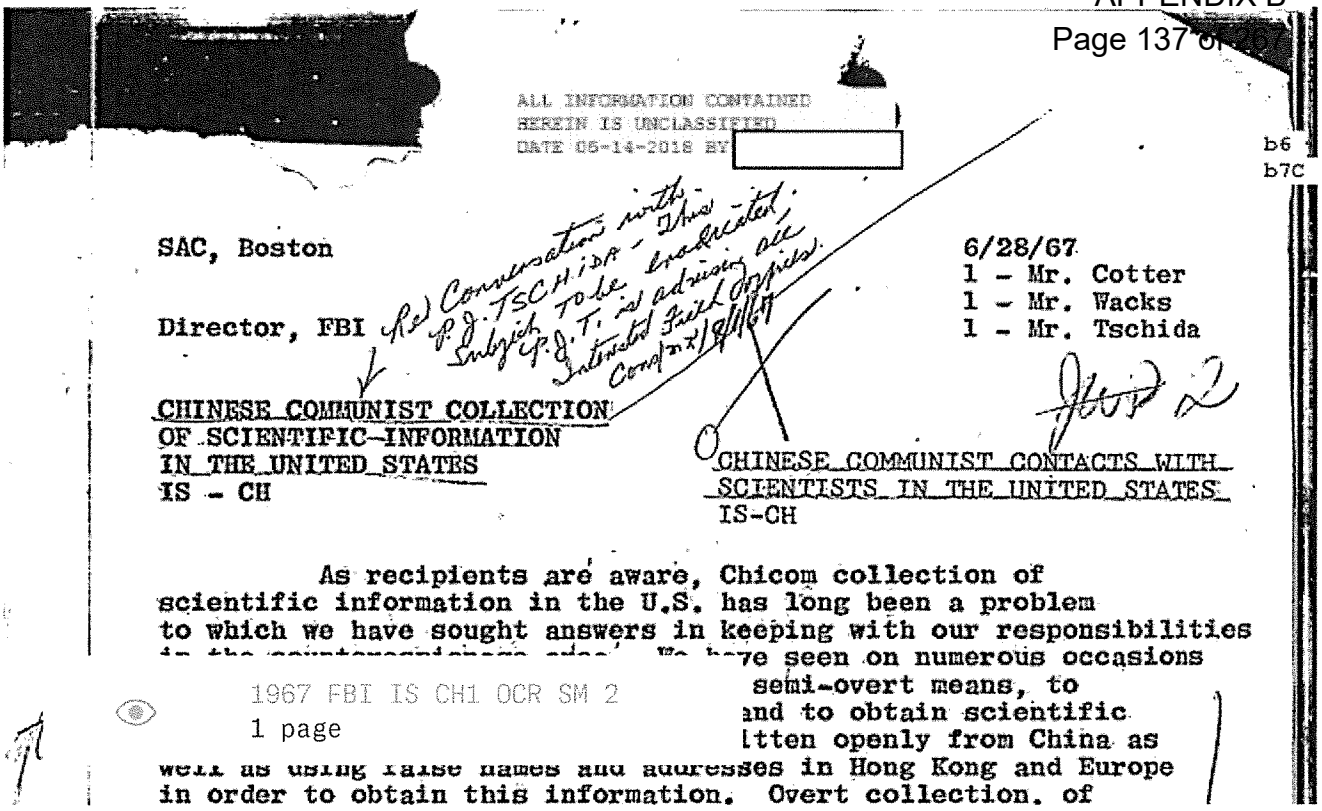
In the wake of the Cultural Revolution, China's Communist leaders were openly courting overseas Chinese scholars, and with his job prospects in America diminished, Tsien tried to leave for China with his family. Worried that he was trying to smuggle out valuable defense information, U.S. immigration agents stopped him at the border. For the next five years, he remained under near-constant FBI surveillance. Finally, in 1955, the United States let him leave. The decision had ominous repercussions. In Beijing, he was given a hero's welcome and put to work on weapons research. In 1966, with Tsien's help, China tested a nuclear-tipped missile. The following year, it stunned the world by testing a hydrogen bomb.

Tsien Hsue-Shen, left, director of Caltech's Jet Propulsion Center, confers with his lawyer, Grant B. Cooper, during his deportation hearing on Nov. 16, 1950. Photo: Bettmann Archive/Getty Images

Tsien's story might have served as a lesson in how suspicion and surveillance can create unnecessary problems. But for Hoover's FBI, his contributions to Chinese defense technology justified escalated surveillance.

Eleven days after China's 1967 weapons test, a memorandum from the FBI director's office arrived in field offices around the country. "The recent detonation of a hydrogen bomb, far ahead of the time the Western intelligence community anticipated China would have such capability, highlights the fact that covert collection of information is undoubtedly going on," the memo read.

That China's weapons knowledge was stolen was not, in fact, a foregone conclusion. Before it severed relations with Beijing in 1960, the Soviet Union had provided critical weapons assistance, and the Chinese nuclear weapons project included a number of skilled scientists besides Tsien. But Hoover suspected espionage — and he had a target group in mind. He warned in a 1966 article of the danger of "persons who have strong ties to the Orient," particularly "students and scientists with living relatives behind the Bamboo Curtain." The 1967 internal FBI memo, which referred to Chinese Communists as "Chicoms," echoed this sentiment. "While it is known that numerous Western-trained scientists, particularly Chinese from U.S., have returned to China and have the training and ability to accomplish a nuclear program," the memo said, "the Chicoms must keep up to date on technological advances in the West in order to create the finished product. We have long suspected that Chicom collection of needed information is accomplished through contacts with ethnic Chinese scientists and technicians in this country." A later program document was more direct, warning bluntly of "the problem of Chinese scientists" in the United States.



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-14-2018 BY [redacted]

b6
b7C

SAC, Boston

Director, FBI

6/28/67
1 - Mr. Cotter
1 - Mr. Wacks
1 - Mr. Tschida

CHINESE COMMUNIST COLLECTION
OF SCIENTIFIC-INFORMATION
IN THE UNITED STATES
IS - CH

CHINESE COMMUNIST CONTACTS WITH
SCIENTISTS IN THE UNITED STATES
IS-CH

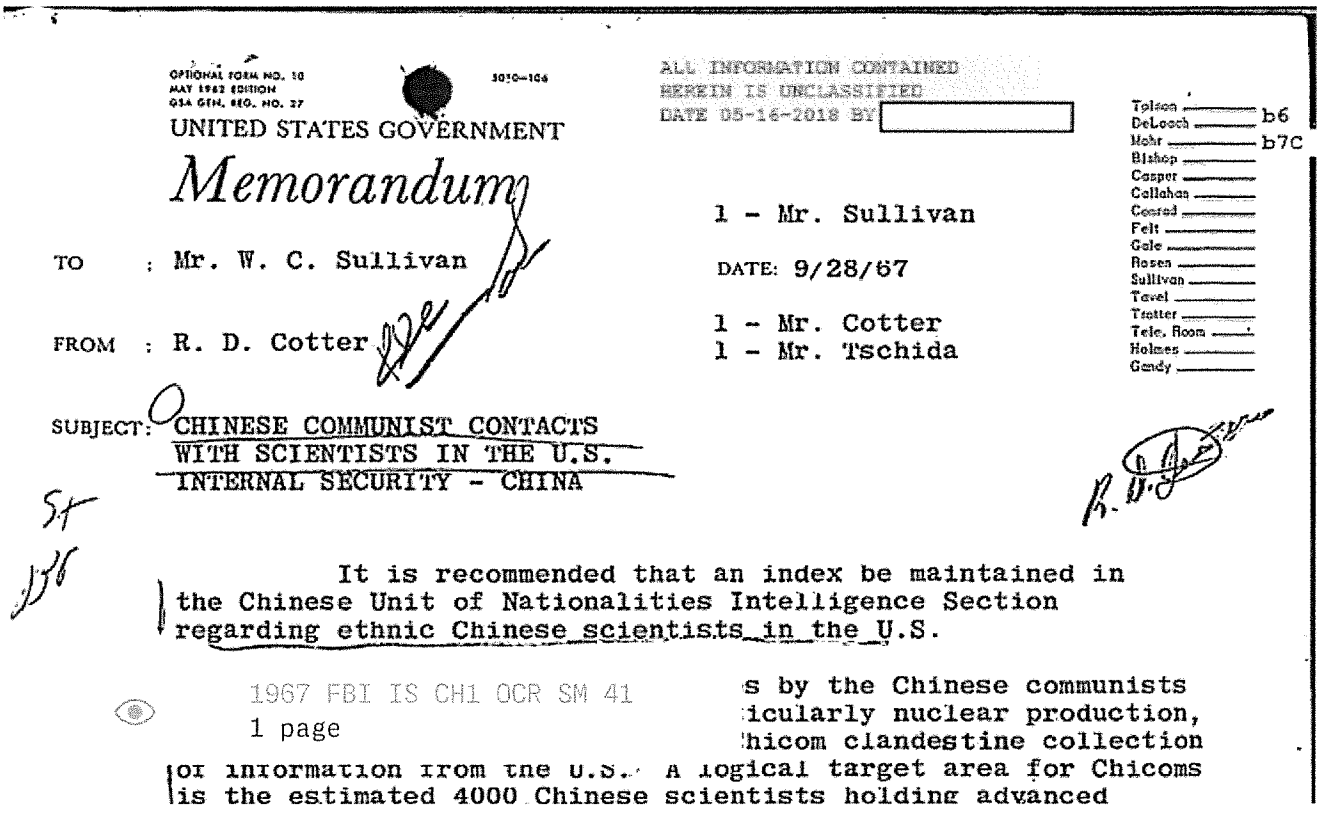
As recipients are aware, Chicom collection of scientific information in the U.S. has long been a problem to which we have sought answers in keeping with our responsibilities
ve seen on numerous occasions
semi-overt means, to
and to obtain scientific
itten openly from China as
well as using false names and addresses in Hong Kong and Europe in order to obtain this information. Overt collection of

1967 FBI IS CH1 OCR SM 2
1 page

Like Sheng, many ethnic Chinese students and scientists in America at the time had emigrated before the 1949 revolution. Others had come from Taiwan and Hong Kong, meaning that they were probably not diehard Communists. But the FBI suspected, citing a confidential source, that scientific secrets were passed to the Chinese government through "networks operating among Chinese communities in this country." To combat this imagined drain of information, Hoover's office proposed compiling lists of ethnic Chinese researchers and students — including U.S. citizens — and placing them under surveillance.

An internal FBI letter sent on September 28, 1967, recommended that "an index be maintained in the Chinese Unit of Nationalities Intelligence Section regarding ethnic Chinese scientists in the U.S." in order to create "a central repository of information" on these individuals. The letter suggested compiling three-by-five index cards listing the profession, clearance level, background, and "degree of cooperation" of each scientist and keeping the cards in a locked drawer. The writer estimated that five people could be added to the index every week. FBI leadership believed that there were 4,000 ethnic Chinese

scientists with advanced degrees working in U.S. universities and industry at the time. (The actual figure may have been higher.)



OPTIONAL FORM NO. 10
MAY 1962 EDITION
GSA GEN. REG. NO. 27
5010-106

UNITED STATES GOVERNMENT

Memorandum

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-16-2018 BY [redacted]

TO : Mr. W. C. Sullivan

FROM : R. D. Cotter

1 - Mr. Sullivan

DATE: 9/28/67

1 - Mr. Cotter
1 - Mr. Tschida

Tolson
DeLoach
Mohr
Bishop
Casper
Callahan
Conrad
Felt
Gale
Rosen
Sullivan
Tavel
Trotter
Tele. Room
Holmes
Gandy

b6
b7C

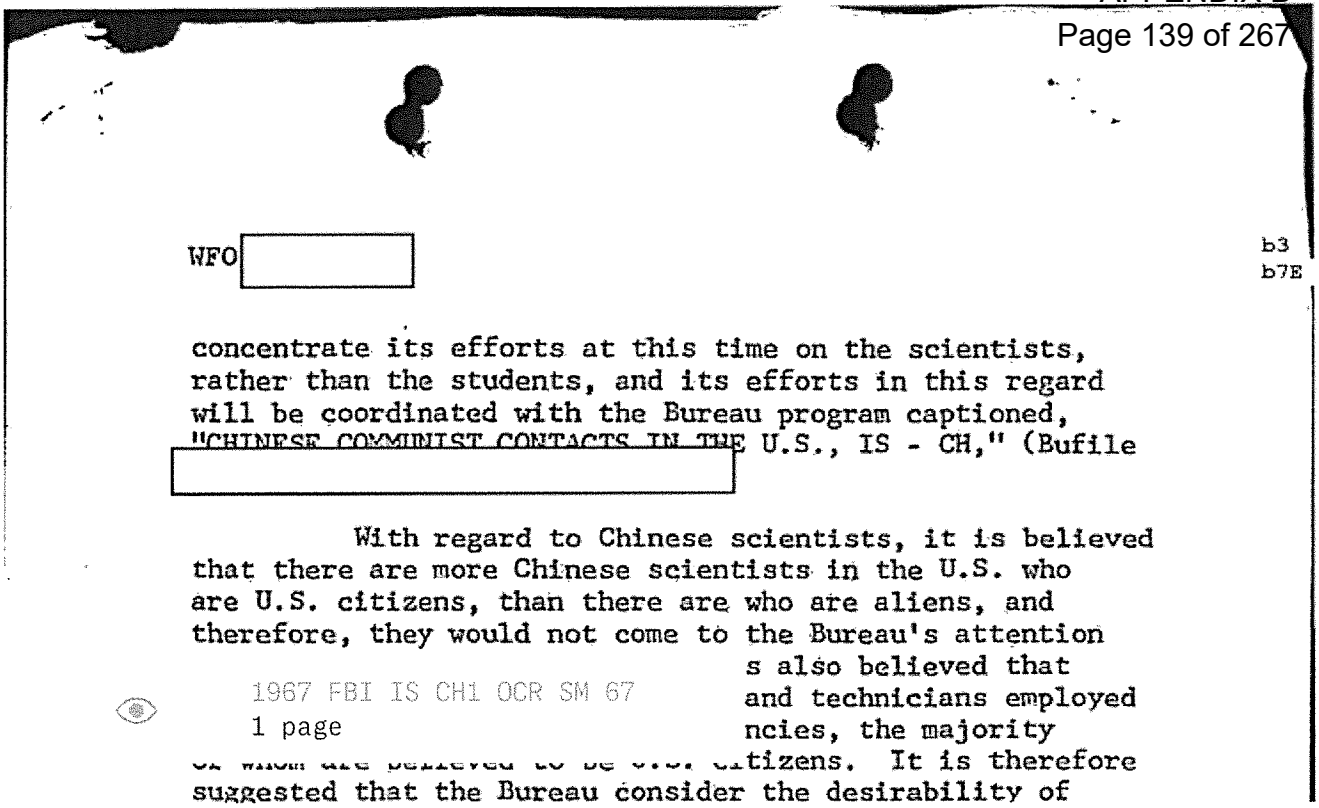
SUBJECT: CHINESE COMMUNIST CONTACTS
WITH SCIENTISTS IN THE U.S.
INTERNAL SECURITY - CHINA

It is recommended that an index be maintained in the Chinese Unit of Nationalities Intelligence Section regarding ethnic Chinese scientists in the U.S.

1967 FBI IS CH1 OCR SM 41
1 page

s by the Chinese communists
icularly nuclear production,
hicom clandestine collection
or information from the U.S. A logical target area for Chicoms is the estimated 4000 Chinese scientists holding advanced

The documents show both that the FBI cast a wide net and that it struggled to come up with useful lists. One document made clear that the bureau aimed to identify U.S. citizens of Chinese descent, not just Chinese nationals. The director's office recommended working off the membership records of the Chinese Association of Scientific Workers, an organization that had ties to the Chinese Communist Party but had disbanded 17 years earlier. "They didn't have any overall information on Chinese scientists in the U.S.," said Wang, the scholar of U.S.-China relations in the Cold War era, "so the best they could come up with was that 1950 list."



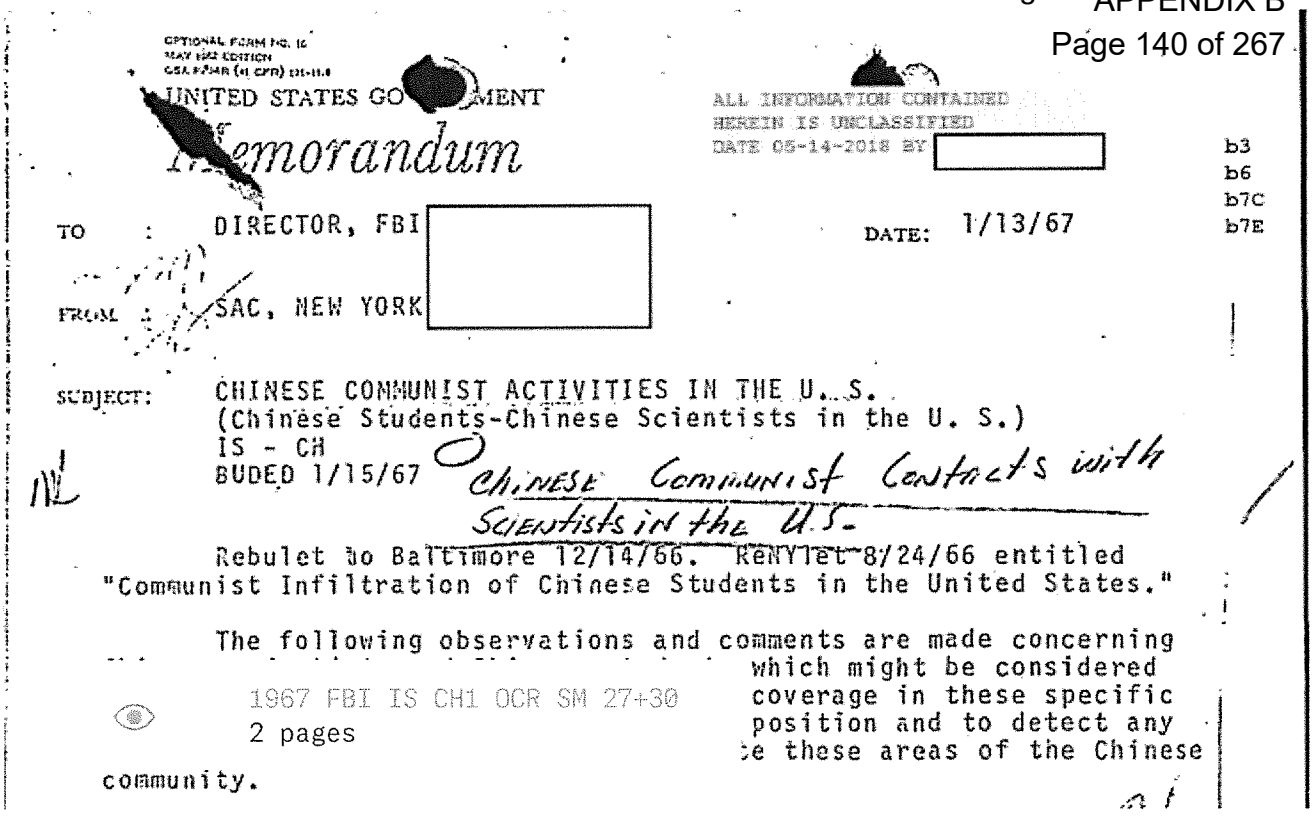
WFO [redacted] b3 b7E

concentrate its efforts at this time on the scientists, rather than the students, and its efforts in this regard will be coordinated with the Bureau program captioned, "CHINESE COMMUNIST CONTACTS IN THE U.S., IS - CH," (Bufile [redacted]

With regard to Chinese scientists, it is believed that there are more Chinese scientists in the U.S. who are U.S. citizens, than there are who are aliens, and therefore, they would not come to the Bureau's attention s also believed that and technicians employed ncies, the majority of whom are believed to be U.S. citizens. It is therefore suggested that the Bureau consider the desirability of

1967 FBI IS CH1 OCR SM 67
1 page

One FBI special agent in charge noted in a response to the director's office that there were some 2,000 ethnic Chinese students in the New York area alone. Foreign student advisers might help identify the most relevant targets, he wrote, but they might not cooperate on such "a sensitive area of inquiry," adding that "conceivably such data could not be obtained directly from certain schools." It was the late 1960s; few people in academia were inclined to cooperate with the FBI. The agent suggested asking defense contractors for lists of ethnic Chinese employees.



OPTIONAL FORM NO. 10
MAY 1962 EDITION
GSA FPMR (41 CFR) 101-11.6

UNITED STATES GOVERNMENT

Memorandum

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-14-2018 BY [redacted]

b3
b6
b7C
b7E

TO : DIRECTOR, FBI [redacted]

DATE: 1/13/67

FROM : SAC, NEW YORK [redacted]

SUBJECT: CHINESE COMMUNIST ACTIVITIES IN THE U.S.
(Chinese Students-Chinese Scientists in the U. S.)
IS - CH
BUDED 1/15/67

Chinese Communist Contacts with Scientists in the U.S.

Rebulet to Baltimore 12/14/66. ReNYlet 8/24/66 entitled "Communist Infiltration of Chinese Students in the United States."

The following observations and comments are made concerning which might be considered coverage in these specific position and to detect any e these areas of the Chinese community.

1967 FBI IS CH1 OCR SM 27+30
2 pages

Nonetheless, the New York field office opened as many as 200 files on ethnic Chinese students in technical fields. San Francisco opened as many as 75 files. Cincinnati and Seattle responded as well. The program documents include several names of targeted individuals, as well as general descriptions of specific targets, like “a graduate student” and “a Chinese engineer at Boeing.” Hoover’s office ordered the file of Tsien Hsue-Shen reopened, and the FBI tracked people with even tenuous connections to the rocket scientist, including his friends’ relatives. One person monitored under the program was an MIT professor from Indonesia — a target, presumably, because he was of Chinese ethnicity.

It is unclear from the documents whether the Chinese scientist program started in 1967 or simply accelerated after the hydrogen bomb test. Sheng first drew the FBI’s notice in 1965, when, according to his file, “he made numerous allegations, both of a criminal and security nature, concerning a former friend who owed him a large sum of money.” (His file does not specify, but Liu believes that these allegations were made to local police.) In any case, by 1967, some agents had ambitious goals for the project. The special agent in charge of the San

Francisco office suggested recruiting ethnic Chinese scientists as potential double agents. This plan involved planting researchers in critical laboratories, then waiting until Chinese intelligence operatives approached them.

Whether the plan was broadly executed or produced useful intelligence is unknown, but at least one Chinese American scientist from the era reported being tasked with spy work. As a physicist at Johns Hopkins University's Applied Physics Laboratory, Chih-Kung Jen often attended international conferences. In his memoir, Jen recalled that ahead of a conference in Tokyo in the late 1960s, a representative from an unnamed agency came to his office and tried to persuade him to spy on a mainland scientist whom Jen considered a friend. "According to his plan, I was to look for a man seated in an airport waiting chair reading a particular newspaper, and to approach this man calling him by the name of 'Mr. Winston,' after which I would receive further instructions," Jen wrote. After the agent concluded his explanation, he pulled out a checkbook, tore off a blank check, and handed it to Jen in an apparent effort to buy the physicist's cooperation. The offer made Jen furious. He insisted that the man get out of his office.

SF [redacted]
BW/cmp

b3
b7E

(1) The Cincinnati Office be furnished the membership list of the CSWA and that these lists be searched [redacted] in order to determine which former members of the CSWA now hold security clearances. Such a procedure should substantially reduce the list of possible suspects as well as furnishing the present location of these individuals.

(2) The Bureau, through liaison with appropriate agencies, would attempt to obtain the following information:

(a) An evaluation of the scientific knowledge of China in 1949 in the field of nuclear

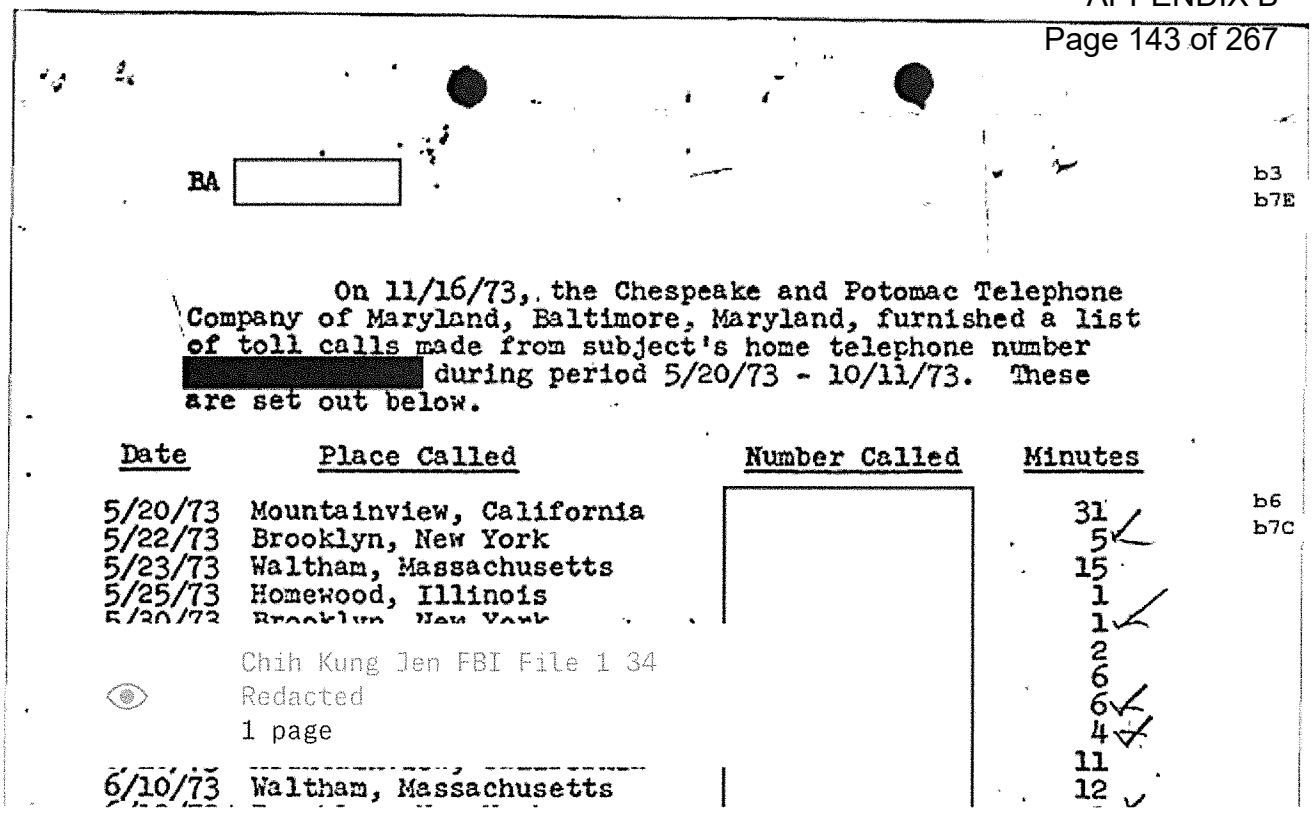
1967 FBI IS CH1 OCR SM 47
1 page

...h Chicom knowledge in the nuclear field could reach through information brought back by scientists returning

After Nixon's historic visit to China, the Chinese scientist program continued. As Chinese American scientists returned to visit long-lost friends and relatives, the bureau closely tracked them.

In 1972, Jen led a delegation of Chinese American scientists and their families to China. Katherine Yih, who joined her father on the trip, recalled a highly orchestrated tour that included visiting agricultural communes and watching children's dance performances. "We were being shown the successes of the revolution," she said. The visitors were seen as important enough that they were also taken to meet Premier Zhou Enlai, a development that almost certainly heightened the suspicions of U.S. counterintelligence operatives.

Jen held a U.S. government security clearance but did not work with classified material. After the trip, his FBI file reveals, the bureau monitored the phone numbers he called, as well as how long he stayed on the phone for each conversation. The file also describes efforts to ascertain his loyalty to the United States.



BA [redacted]

b3
b7E

On 11/16/73, the Chesapeake and Potomac Telephone Company of Maryland, Baltimore, Maryland, furnished a list of toll calls made from subject's home telephone number [redacted] during period 5/20/73 - 10/11/73. These are set out below.

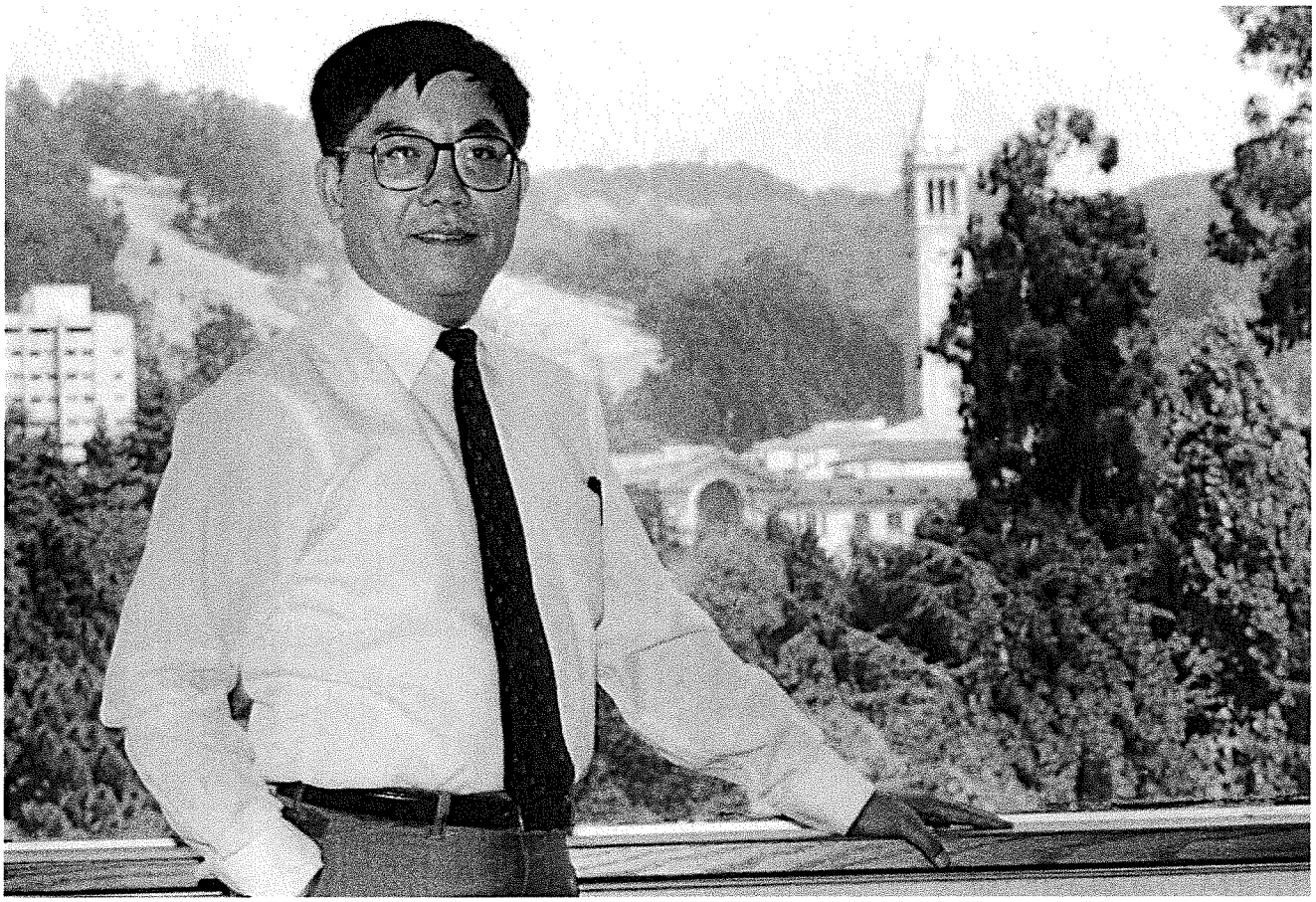
Date	Place Called	Number Called	Minutes
5/20/73	Mountainview, California	[redacted]	31
5/22/73	Brooklyn, New York		5
5/23/73	Waltham, Massachusetts		15
5/25/73	Homewood, Illinois		1
5/30/73	Brooklyn, New York		1
	Chih Kung Jen FBI File 1 34		2
	Redacted		6
	1 page		6
			4
			11
6/10/73	Waltham, Massachusetts		12

b6
b7C

According to a 1975 document listing all domestic FBI counterintelligence programs, the Chinese scientist program was focused on recruiting scientists as assets. Paul Moore, a former FBI China analyst who started at the bureau in the late 1970s, explained the program in an interview as an attempt to work counterintelligence in a difficult situation. "The guys in the Chinese squad had to do something, so what were they going to do? There wasn't any Chinese diplomatic establishment, China was thousands of miles away, and they didn't want to say, 'We're not doing anything about China.' So what's left? You've got the well-educated Chinese, and you've got the Chinese coming into the country illegally."

Moore told me that he believed the program was scrapped in the late 1970s. The last document clearly connected to the Chinese scientist program that I could find was from 1978. But the surveillance of Chang-Lin Tien, the professor of mechanical engineering at UC Berkeley who later became the university's chancellor, continued into the 1980s. His FBI file, published in 2012 by the Daily Californian, shows that agents followed him to art openings, pulled his credit reports, and called

hotels he had booked to make sure he checked in. (The bureau also tried, unsuccessfully, to recruit him as an informant.) A gregarious man who once led a conga line at the wedding of two of his students, Tien enjoyed hosting visitors from around the world and believed in building ties with China. But he made clear that he saw the FBI's efforts as harassment. "He expressed his belief that the FBI was continuing to harass Chinese academicians like himself just as was done during the 1950s," according to a note in his file.



Chang-Lin Tien, chancellor of the University of California at Berkeley, in 1990 on the Berkeley campus. Photo: Kristy MacDonald/AP

Melany Hunt, a scientist who was a Ph.D. student in Tien's lab in the 1980s, said that the work she and others conducted there was all basic research. "My grandfather always believed cooperation in the sciences could play a key role in promoting peace between the U.S. and China," Tien's granddaughter, Kylie Tien, told me. "That aspiration put him

under the scrutiny of a program launched at a time in history where fear and suspicion heavily impacted our government's actions."

In 1996, Tien appeared on President Bill Clinton's shortlist for secretary of energy. The post would have made him the first-ever Asian American cabinet secretary. But he became an undeserving casualty in the "Chinagate" campaign finance scandal, an alleged effort by China to influence U.S. politics, and was abruptly dropped as a candidate. (Clinton later appointed him to the National Science Foundation board.)

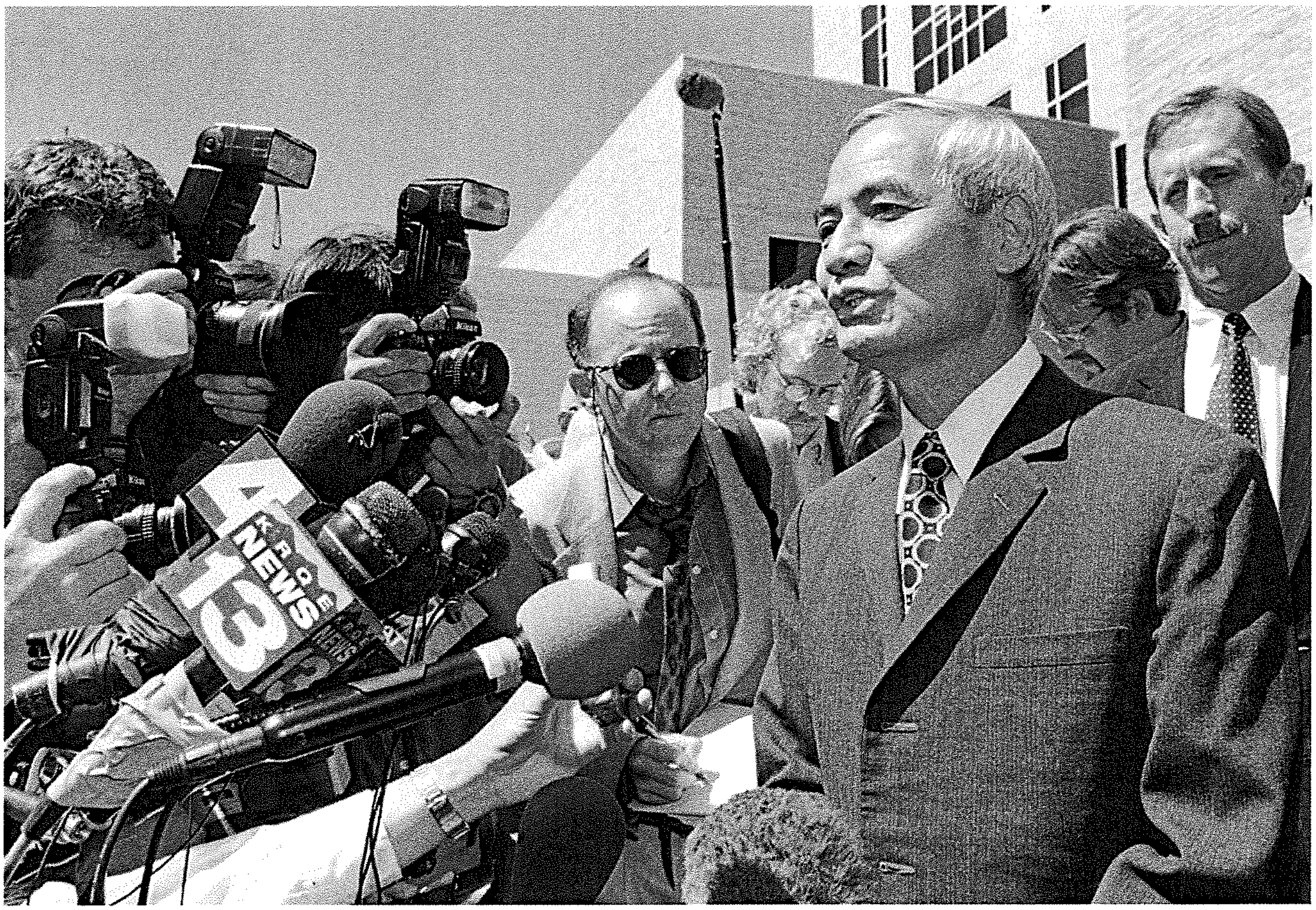
The logic underlying the Chinese scientist program drove FBI investigations for years. In 1995, history repeated itself when a defector claiming to have worked on China's weapons program turned up at the offices of Taiwan's internal security service, carrying documents indicating that China had some knowledge of the United States's W88 warhead. As in 1967, some in Washington suspected foul play. The only possible explanation, they concluded, was that China had stolen weapons secrets from the United States. Deciding that the leak must have come from Los Alamos National Laboratory, Department of Energy investigators went in search of a suspect. The FBI was enlisted to help.

The bureau codenamed the inquiry Kindred Spirit, after China's assumed tendency to target ethnic Chinese. Investigators homed in on ethnic Chinese researchers who had worked in any way on the development of the warhead. They soon found a suspect in a longtime Los Alamos scientist: Wen Ho Lee. In a strange twist, Lee's wife Sylvia, had reportedly acted as an asset for the FBI and CIA in the 1980s. Now they were on the other side. Before Lee could be formally charged, someone leaked his name to the New York Times, which outed him as a suspect in March 1999.

To justify searching Lee's home, the FBI submitted an affidavit that used language drawn from Hoover's playbook, noting that "People's Republic of China intelligence operations virtually always target overseas ethnic

Chinese with access to intelligence information sought by the PRC." Lee was arrested in December 1999 and held in solitary confinement 23 hours a day in a New Mexico jail for the better part of a year.

Eventually, the case against Lee unraveled and in September 2000, he was acquitted of 58 of the 59 charges against him. He pleaded guilty to a single felony count of mishandling classified information. In 2006, Lee won a $1.6 million settlement from the U.S. government and five media organizations.



Former Los Alamos nuclear scientist Wen Ho Lee, right, addresses media outside the Federal Courthouse in Albuquerque, N.M., on Sept. 13, 2000, after he was freed from nine months of solitary confinement. Photo: Mike Fiala/AFP via Getty Images

The Lee debacle prompted a congressional investigation and sparked a national conversation. Nonetheless, stereotyping and bad analysis endured within the FBI. Moore, the former analyst, popularized a theory

known as "a thousand grains of sand," which held that China used a "human wave" of ethnic Chinese intelligence collectors to pursue bits of information that the government then pieced together. "The myth that Chinese Americans are more susceptible to becoming Chinese agents is persistent," said former FBI agent Michael German, a fellow with the Brennan Center for Justice's Liberty and National Security Program. He compared it to the tendency in counterterrorism work to blur "important distinctions between nationality, sects, or ambitions of different groups into one Muslim radicalism." He added: "Prioritizing national security augurs this kind of bias."

The same bias extends to the treatment of Chinese American FBI employees, critics say. Despite efforts from FBI leadership to diversify the bureau's staff and calls from community organizations to increase representation of people of color, Asian Americans now make up only about 4 percent of agents. A former FBI supervisor whom I'll call Don Lieu told me that in a routine security check, his unit's embedded security officer asked him whether he hung Chinese lanterns in his home and whether he was friendly with people who were "in touch with Chinese culture." (Lieu asked me to identify him by his grandfather's first name and a family surname, citing concerns about retaliation.) Another time, he said, a security officer brought up the fact that Lieu dated Asian Americans. Lieu, who grew up in the New York City area, said he responded, "I can guarantee that none of these women are foreign nationals. In some cases, they are multigeneration Americans like myself." He told me that the security officer then questioned how he could be sure that a girlfriend was a U.S. citizen, suggesting that any "close and continuing contact" with a Chinese American woman put the United States at risk.

Lieu told me that in his view, institutional racism, not individual bias, is to blame for these encounters. "Most of the people who are doing the investigations are just following the guidance of the top boss," he said.

"Everything is coming down, and they're just getting their marching orders to do this." The message from leadership, he said, is that "Chinese Americans are being weaponized as a tool by foreign nationals."

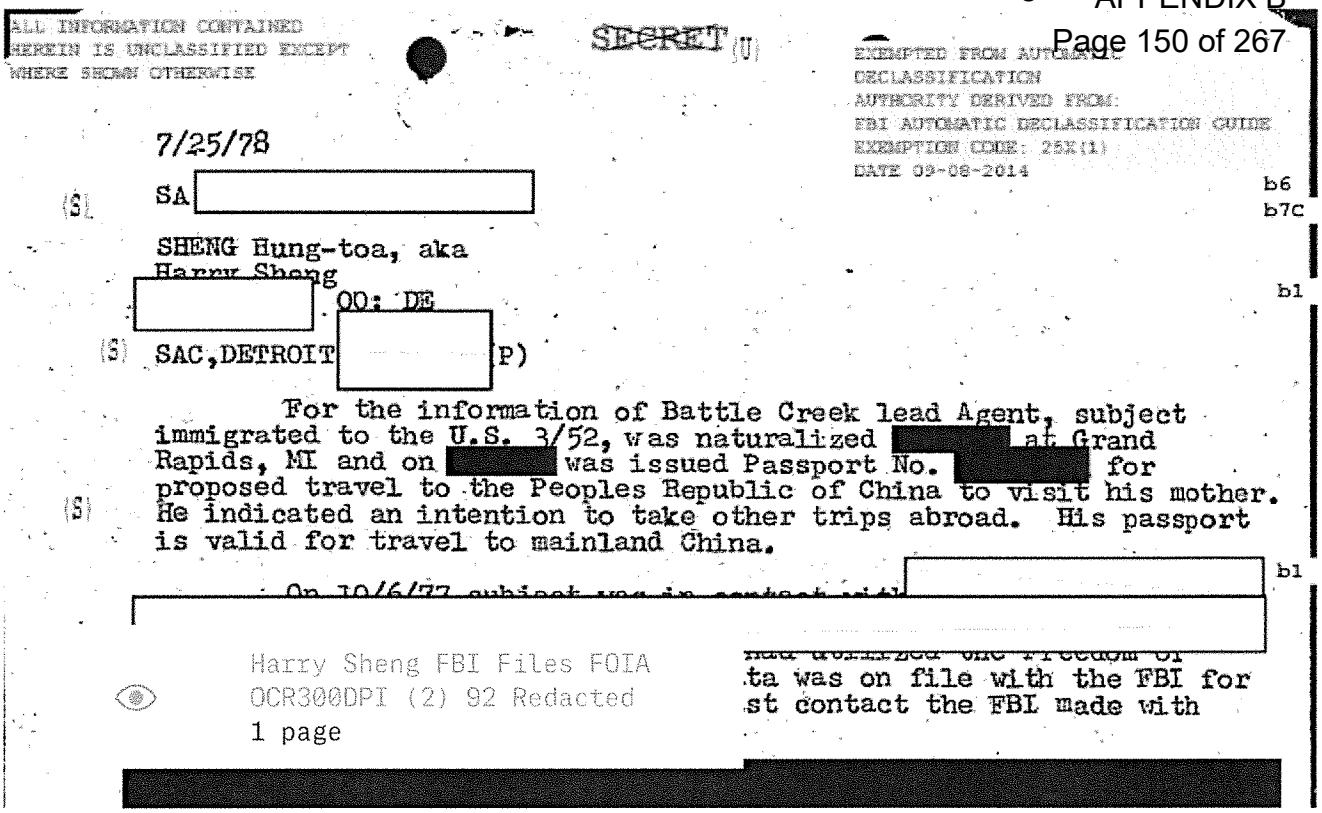
FBI training materials obtained by the American Civil Liberties Union under the Freedom of Information Act in 2012 reveal approaches that are at best inadequate and at worst offensive. One presentation is sourced from "The Idiot's Guide" — presumably "The Complete Idiot's Guide to Modern China" — and titled "The Chinese."

"Imagine trying to explain the behavior of Americans and titling a slide presentation 'The Americans,'" said German. "'This is what the Americans are like.' It would be absurd. It's just mind-numbingly stupid to put on a presentation like that."

Another presentation given by the FBI's Behavioral Science Unit, according to the documents obtained in 2012, deals with group-focused cultures, defined as Arabs, Iranians, Koreans, and Chinese. "Never attempt to shake hands with an Asian; never stare at an Asian," the presentation warns. It also contains an offhand reference to "somatization" — the tendency to experience emotional distress as physical pain. The slide offers no explanation, but this idea has been used to suggest that Chinese culture is psychologically immature.

Harry Sheng was an early victim of FBI discrimination. Throughout the 1970s, he kept trying to figure out why his life in the United States had changed so radically after his visit to China. "I contributed my best knowledge to the U.S. defense work," he wrote his congressperson, Milton Robert Carr of Michigan, in 1975. "I will continue to fight until the truth comes out." When Carr asked the FBI for details, the bureau replied in a letter: "FBI files contain no derogatory information on Mr. Sheng."

In 1977, Sheng applied for a new passport, explaining that he wanted to visit his mother again. Later in the year, he corresponded with a source whom the FBI considered suspicious — the person's name is redacted — and submitted a FOIA request for his FBI file. In response, the FBI pulled his driver's license and bank and income tax records and followed him around Michigan. By then, Sheng could find only temporary jobs. He started a stint at McGraw-Edison, which manufactured heating and air-conditioning units. The FBI monitored his residence and tailed his red Volkswagen as he drove from his home to work one morning at 7:15 a.m., according to a report that appears in his FBI file.



ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

SECRET (U)

EXEMPTED FROM AUTOMATIC DECLASSIFICATION
AUTHORITY DERIVED FROM:
FBI AUTOMATIC DECLASSIFICATION GUIDE
EXEMPTION CODE: 25X(1)
DATE 09-08-2014

7/25/78

(S) SA [redacted]

b6
b7C

SHENG Hung-toa, aka
Harry Sheng

[redacted] OO: DE

b1

(S) SAC, DETROIT [redacted] (P)

For the information of Battle Creek lead Agent, subject immigrated to the U.S. 3/52, was naturalized [redacted] at Grand Rapids, MI and on [redacted] was issued Passport No. [redacted] for proposed travel to the Peoples Republic of China to visit his mother. (S) He indicated an intention to take other trips abroad. His passport is valid for travel to mainland China.

[redacted] b1

On 10/6/77 subject was in contact with [redacted]

[redacted]

Harry Sheng FBI Files FOIA
OCR300DPI (2) 92 Redacted
1 page

[redacted] had utilized the Freedom of [illegible]ta was on file with the FBI for [illegible]st contact the FBI made with

[redacted]

Thirteen years had passed since Sheng had first appeared on the FBI's radar. He still had no explanation for why he was being watched. A few months later, a confidential memo from the Detroit field office to the director's office stated that there was no "security risk on the part of the subject." The memo concluded: "Detroit is recommending he not be reinterviewed and is closing this file."

CONFIDENTIAL

DE [redacted] (C) b1

Investigation verified his address as being [redacted], his former employment with Sparton Corporation, Jackson, Michigan, and his employment with McGraw-Edison Company, Albion, Michigan was verified. His usual occupation is engineer-draftsman. His passport file contained a request by subject, under the Freedom of Information/Privacy Acts dated 12/16/77, regarding investigation of him, apparently objecting to an FBI inquiry with his employer. (C) (U)

Review of the files regarding subject, current
d information available
o significant data [redacted] b7E
or security risk on the
fy his being interviewed a
recommending he not be
reinterviewed and is closing this file. (C) (U)

Harry Sheng FBI Files FOIA
OCR300DPI (2) 83 Redacted
1 page

After the Shengs moved to California, they lived a quiet life. Harry Sheng wrote poetry; he gained a reputation in his adopted family for driving at excruciatingly slow speeds and falling asleep during church sermons. He loved his mother, the woman whose illness had brought him so much scrutiny, to the end. Sheng died in 2011. Even in his final years, Liu told me, he would occasionally cry out, “Dear Momma!”

WAIT! BEFORE YOU GO on about your day, ask yourself: How likely is it that the story you just read would have been produced by a different news outlet if The Intercept hadn't done it?

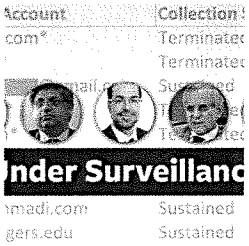
As the pandemic worsens, it's not just the virus itself that threatens human life. The corruption, cronyism, and incompetence of those in power is adding fuel to the fire. The public deserves to know more than just case counts and death tolls, which is why our reporters are digging deep to break stories on corporate profiteering and political jockeying that undermine public health.

The kind of reporting we do is essential to democracy, but it is not easy, cheap, or profitable. The Intercept is an independent nonprofit news outlet. We don't have ads, so we depend on our members — 55,000 and counting — to help us hold the powerful to account. Joining is simple and doesn't need to cost a lot: You can become a sustaining member for as little as $3 or $5 a month. That's all it takes to support the journalism you rely on.

Become a Member →

RELATED

The FBI Has a Long History of Treating Political Dissent as Terrorism



Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On

FBI Tracked an Activist Involved With Black Lives Matter as They Traveled Across the U.S., Documents Show

The FBI Tried to Use the #MeToo Moment to Pressure an Environmental Activist Into Becoming an Informant

LATEST STORIES

Amid Protests, Phoenix Police Swept Up Immigrants on Mistaken Charges. Now They Face Deportation.

Hannah Critchfield — 11:42 a.m.

"This is a prime example of why local law enforcement should not have any interaction with ICE — because cops make mistakes," a Phoenix attorney said.

The Coronavirus Stimulus Discourages Aid to Small Business Owners With a Criminal Record

Bryce Covert — 6:00 a.m.

The Paycheck Protection Program, created by Congress through the CARES Act, is disqualifying and discouraging small business owners with felony convictions.

Hickenlooper, Champion of "Broken Windows" Policing, Says "Every Life Matters" in Response to Protests

Akela Lacy, Aída Chávez — Jun. 7

John Hickenlooper, recruited and backed by Democratic leaders in Washington for a Colorado Senate seat, faces questions about his policing approach as Denver mayor.

The Intercept_

ABOUT
EDITORIAL POLICIES
BECOME A SOURCE
JOIN NEWSLETTER
BECOME A MEMBER
TERMS OF USE
PRIVACY
SECUREDROP

© FIRST LOOK MEDIA. ALL RIGHTS RESERVED

SCMP.COM

South China Morning Post

Post Magazine / Long Reads

Spying charges against Chinese-American scientists spark fears of a witch hunt

A number of those accused have had their cases dropped abruptly, but the damage to their reputations and careers has already been done

Topic | US-China relations

MARA HVISTENDAHL

Published: 10:00pm, 5 May, 2018

Why you can trust SCMP

Just after dawn on May 21, 2015, physicist Xiaoxing Xi awoke to find a dozen or so armed federal agents swarming his home in the suburbs of Philadelphia, Pennsylvania, in the United States. When he rushed to open the door, the agents drew their guns and announced that they had a warrant for his arrest. They had brought along a battering ram.

The night before, Xi's wife had returned from a conference overseas. The couple had stayed awake chatting with their daughters, planning a family outing to a popular Korean barbecue restaurant to eat fried chicken. Now his daughters – one in middle school, the other in college – watched in horror as agents handcuffed Xi, who was still not fully dressed, and escorted him away.

Chinese American scientists reveal agony of being accused by US of passing secrets to China as charges are dropped

Then interim chairman of the physics department at Philadelphia's Temple University, Xi is a naturalised US citizen who has lived and worked in the country since 1989. He is among the world's leading experts on superconducting thin films, which carry electricity without resistance at very low temperatures. At the time of his arrest, he was in what he calls a "very productive" phase of his career, overseeing nine research projects, including work for Temple University's Energy Frontier Research Center, which is funded by the US Department of Energy.

But now he stood charged with trying to transfer to China designs for a proprietary technology – specifically for a device called a pocket heater, produced by Superconductor Technologies Inc (STI) of Austin, Texas, which makes thin films of the superconductor magnesium diboride.

Xi faced 80 years in prison and a US$1 million fine.

He was released after putting up his home as bail, but his passport was confiscated and his domestic travel restricted to eastern Pennsylvania. For days, his family avoided the windows in their home as television stations broadcast live from their front garden. Over the months that followed, they drained their bank accounts to pay legal fees.

Citing a non-disclosure agreement that Xi had signed in 2006, to conduct research with a pocket heater, the US attorney's office in Philadelphia had charged him with four counts of wire fraud, for four emails sent to contacts in China about establishing labs and a collaboration involving a thin film deposition device. But on September 11, 2015, before a trial date had been set, the US attorney's office abruptly dropped the charges, noting that "additional information came to the attention of the government".

I was charged for things that were just normal collaborations. If all these normal activities could be seen as

people through the wringer

Brian Sun, trial lawyer

A growing number of scientists have been targeted improperly as US Department of Justice (DOJ) lawyers have stepped up prosecutions, advocates say. Since 2014, charges have been dropped against at least five Chinese-born scientists accused of crimes related to secrets, theft or economic spying. A sixth defendant, a New York University medical-imaging researcher, accused of passing confidential information about magnetic resonance imaging (MRI) technology to a company in China, pleaded guilty to a single misdemeanour. In several instances, critics say, the US government has charged scientists without understanding the science at the heart of its allegations.

Xi's case, which was overseen by FBI Special Agent Andrew Haugen, is emblematic. Court documents state that "the government seized extensive electronic evidence and searched multiple hard drives" in the process of investigating Xi. But prosecutors apparently did not consult technical experts before issuing the indictment, says Nelson Dong, a former DOJ official and a lawyer, who was not involved in Xi's case. "That suggests to me that people really did rush to judgment," he adds. "They saw red, so to speak."

The prosecutions have spooked many Chinese-American scientists, who fear that any collaboration with Chinese nationals will invite suspicion.

criminal activities, then the environment is quite frightening
Xiaoxing Xi, physicist

At issue, Xi's lawyer and scientists familiar with the case assert, was a glaring misinterpretation of the science involved. The devices Xi had discussed with Chinese colleagues were not the pocket heater, they say, and the exchanges posed no threat to American interests.

"The whole case against Xiaoxing Xi was just completely misconceived," says David Larbalestier, a physicist at Florida State University, Tallahassee, who submitted an affidavit for his defence.

Together with cybercrime, economic espionage and the theft of trade secrets are now priorities for the Federal Bureau of Investigation (FBI). The bureau's dedicated economic espionage unit was established in 2009. Since then the number of cases it handles – most of them involving China – has grown by an average of 18 per cent year on year. The FBI has simultaneously pursued an ambitious public awareness campaign around the issue, centred on a dramatic film depicting a Chinese company attempting to steal trade secrets from a US competitor.

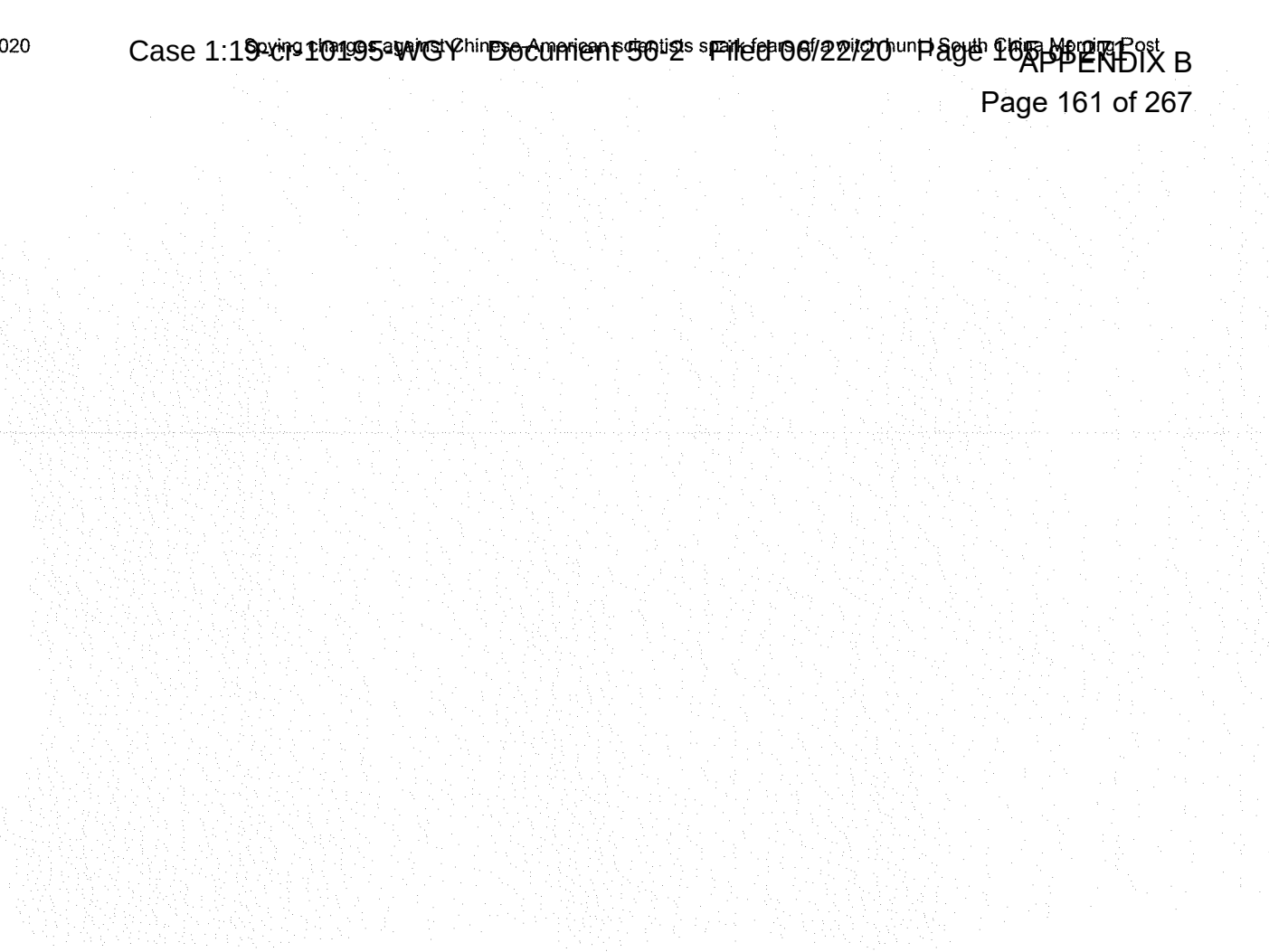
The Company Man: Protecting America's Secrets

In February, FBI director Christopher Wray asserted at a Senate Intelligence Committee hearing that spying by Chinese professors, scientists and students in the US constituted a "whole-of-society threat", adding, "It's not just in major cities; it's in small ones as well; it's across basically every discipline."

US President Donald Trump, who rarely agrees with the FBI, has also highlighted intellectual property (IP) theft by China as a top concern. Last year, he directed US Trade Representative Robert Lighthizer to initiate an investigation into Chinese trade practices, including IP theft. Results of that investigation, announced in a critical, 81-page report on March 22, contributed to mounting trade tensions between the US and China.

Trump cited the IP violations outlined in the report as justification for US$50 billion worth of proposed tariffs on Chinese goods. China, in turn, hit back with its retaliatory tariffs on US goods. The two sides have been in trade talks in Beijing in recent days. Earlier this week, *The New York Times* reported that the White House was discussing measures to block Chinese citizens from undertaking sensitive research in US universities over fears they may be acquiring intellectual secrets, and that these might include restrictions on certain types of visa.

Yes, America has a legitimate concern about cyber hacking and trade secrets theft. But [...] do your homework. Get the science right before you put these



Xi with Xiafen "Sherry" Chen during a press conference in Washington, in 2015. Picture: AFP

In 2015, following the sudden dismissal of charges against National Weather Service (NWS) hydrologist Xiafen "Sherry" Chen, who had been accused of passing information about US dams to a Chinese official, 22 members of Congress signed a letter requesting an investigation into whether federal employees were being racially targeted. The office responded in a letter that "no policy exists of using race or any other civil rights classification" to single out federal employees for arrest or scrutiny.

But Wray's comments in February have brought the issue back into the spotlight. On March 1, a coalition of civil society groups sent Wray a joint letter expressing their concern over his testimony and requesting a meeting to discuss the issue. After the September 11 attacks, the letter noted, FBI and law enforcement groups "reached out to Arab American and Muslim American communities to ensure everyone came together in unity". Now, at another moment of heightened tension, the groups have urged authorities to reach out to Asian Americans.

Leaders in China and US must set clear rules on espionage

In a recent statement, Representative Ted Lieu, a California Democrat, said Wray's comments "feed into the false and harmful narrative that somehow Chinese-Americans are more suspicious".

Xi's crime was, according to one legal blog, "emailing while Chinese-American".

The theft of scientific secrets is as old as science itself. Centuries ago, for example, a young US depended greatly on know-how spirited out of Britain, showering accolades on those who stole designs for textile machinery.

Imperial China was a frequent victim as well, with Western powers stealing its methods of porcelain and tea production. But some argue that the past few decades have marked the dawn of a new era, with everything from sensitive military technology to lucrative agricultural secrets now prized spoils.

"As the world becomes more advanced, technology just becomes worth more," says Peter Toren, a former federal prosecutor and a litigator who specialises in trade secrets cases. "Developing countries and companies in developing countries can save hundreds of millions of dollars in research costs by stealing new technology."

FBI director Christopher Wray. Picture: AFP

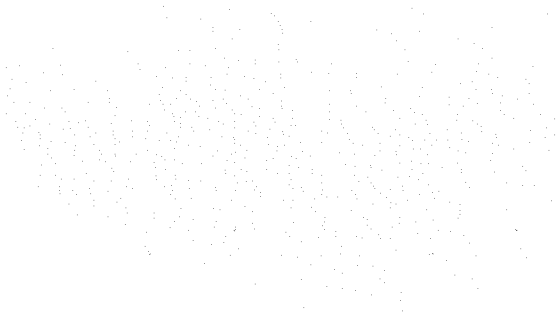
Developing countries are hardly the only perpetrators. In a secret report leaked by Edward Snowden in 2014, the US National Security Agency outlined possible scenarios for cyber operations against foreign research centres, with the aim of capturing knowledge that "would be useful to US industry". And as late as the 1990s, France and Israel were among the world's most prominent industrial spies.

But the US government now sees China as the major foreign threat. Many of the indictments brought under the Economic Espionage Act since its passage, in 1996, have involved China.

In some cases, US prosecutors have assembled reams of evidence. In 2010, Boeing engineer Dongfan Chung – a naturalised American citizen who was born in mainland China and grew up in Taiwan – was sentenced to 15 years in prison for stealing trade secrets connected to the US Space Shuttle programme and Delta IV rocket on behalf of China. When agents raided Chung's home, they found more than 250,000 sensitive documents from defence contractors, some of them hidden in crawl spaces under the house. The FBI alleged that documents in the stash showed Chung was acting at the direction of China's Civil Aviation Administration.

US convicts two of selling DuPont trade secrets to Chinese state-owned firms

Another successful prosecution came in 2014, when entrepreneur Walter Lian-Heen Liew was sentenced to 15 years for conspiring to steal secrets related to titanium dioxide production from DuPont and sell them to state-owned companies in China. (Former DuPont engineer Robert Maegerle was also convicted in the case.)



Former federal prosecutor and a litigator, Peter Toren.

But a startling number of cases have unravelled. In 2014, the US government dropped charges against two former Eli Lilly scientists in Indiana. The attorney's office in Indianapolis had alleged that Guoqing Cao and Shuyu Li, both naturalised US citizens and senior biologists at Eli Lilly, passed research on tailored therapies for cancer and drugs to treat diabetes, obesity and other metabolic disorders to Chinese company Jiangsu Hengrui Medicine.

The case invited heated rhetoric, with a government prosecutor labelling the defendants traitors in an early bail hearing and the defence in its filings invoking the 1954 anti-communist senate hearings convened by then-senator Joseph McCarthy. From October 2013 to November 2014, the two scientists were variously jailed, locked down in a halfway house and kept in round-the-clock home detention.

Yet case documents submitted by Cao's lawyers claim that the trade secrets he allegedly stole had all appeared in published papers years earlier, and that the information did not include drug molecules, formulas or data owned by Eli Lilly. In December 2014, several weeks after a judge agreed to release the researchers, the US attorney's office dropped the charges entirely, citing its "ongoing evaluation and assessment of this case".

Chinese-born professor sues FBI agent over arrest and false espionage accusation

Then, in March 2015, the US government dropped charges against Chen, the NWS hydrologist. Peter Zeidenberg, a partner at law company Arent Fox in Washington, who represents both Chen and Xi, says she merely sent a Chinese official (a former classmate whom she had contacted as a favour to her nephew) links to publicly available websites, including that of the National Oceanic and Atmospheric Administration (NOAA).

The official was tasked with planning repairs for China's reservoirs and had asked Chen how such repairs were funded in the US. Chen referred the official to a division head at the US Army Corps of Engineers, with whom she had worked on projects in the past, Zeidenberg says.

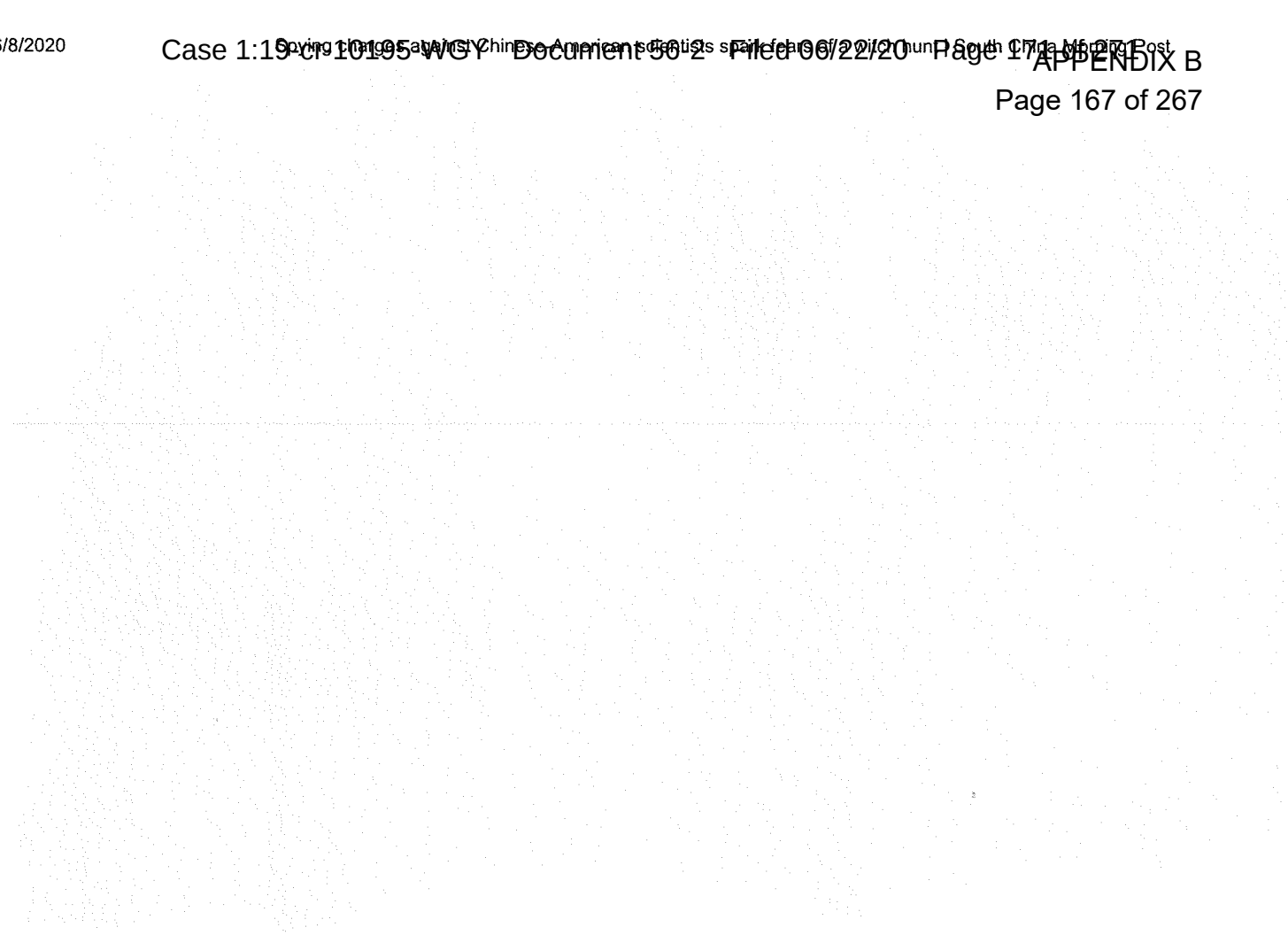
"Why would she be giving her contact in China the phone number of her boss and saying, 'Call her if you have any further questions'? It was absurd," he argues.

Chen was subsequently fired. She sued, alleging employment discrimination. On April 27, a judge ruled in her favour, ordering that Chen be reinstated with back pay.

We need a set of well-defined rules. The indictments have instilled a great deal of uncertainty and anxiety in our community. People are wondering, 'Is this going to happen to me?'
Albert Chang, physicist

Last June, prosecutors brought a case against another NOAA employee: leading climate scientist Chunzai Wang. Charged with eight felony counts, Wang was accused of accepting money from Chinese organisations in violation of US government policy. Ultimately, Wang pleaded guilty to only one count of illegally supplementing his government salary with money received from the Changjiang Scholars Program, which is overseen by China's Ministry of Education. The other charges against him were dismissed. In February, Judge Cecilia Altonaga sentenced him to a single night in jail.

As a result of his conviction, Wang, who is a US citizen, lost the right to vote, to hold office and to possess firearms. In delivering her judgment, Altonaga said that while the scientist made mistakes, it was unfortunate that the issue had not been resolved through other means, implying that his crime was minor enough not to require a federal court hearing. "My only regret [...] is that I have to adjudicate Mr Wang," she said.



US Trade Representative Robert Lighthizer. Picture: Bloomberg

Xi, now 60, was born in Beijing and came of age during the Cultural Revolution. As a teenager, he was sent to the countryside, where he spent several years working in the fields and shovelling pig manure. After the Cultural Revolution ended, in 1976, Xi won admission to Peking University. He went on to earn a PhD before leaving for the US in 1989.

In 1995, he joined the faculty at Pennsylvania State University, University Park campus, where his wife, physicist Qi Li, still teaches.

Before the agents pounded on his door and turned his life upside down, Xi oversaw a team of 16 students and researchers at Temple University and received more than US$1 million a year in research funding. The group had just obtained what Xi calls "breakthrough results" in two areas that they planned to submit to respected journals *Science* and *Nature*. Xi "is among the best thin-film physicists around", says physicist Paul Chu, of the University of Houston in Texas, who submitted an affidavit in his defence. After the indictment, Temple placed Xi on administrative leave.

According to affidavits submitted in the case, the allegations centre on Xi's collaboration with the Shanghai Institute of Applied Physics and Peking University. The indictment alleged that Xi "repeatedly reproduced, sold, transferred, distributed, and otherwise shared" the STI pocket heater with these institutions and then pursued "lucrative and prestigious appointments" in exchange for his assistance. Zeidenberg says Xi never profited financially from the interactions highlighted by the US government.

As the world becomes more advanced, technology just becomes worth more. Developing countries and companies in developing countries can save hundreds of millions of dollars in research costs by stealing new technology
Peter Toren, former federal prosecutor and litigator

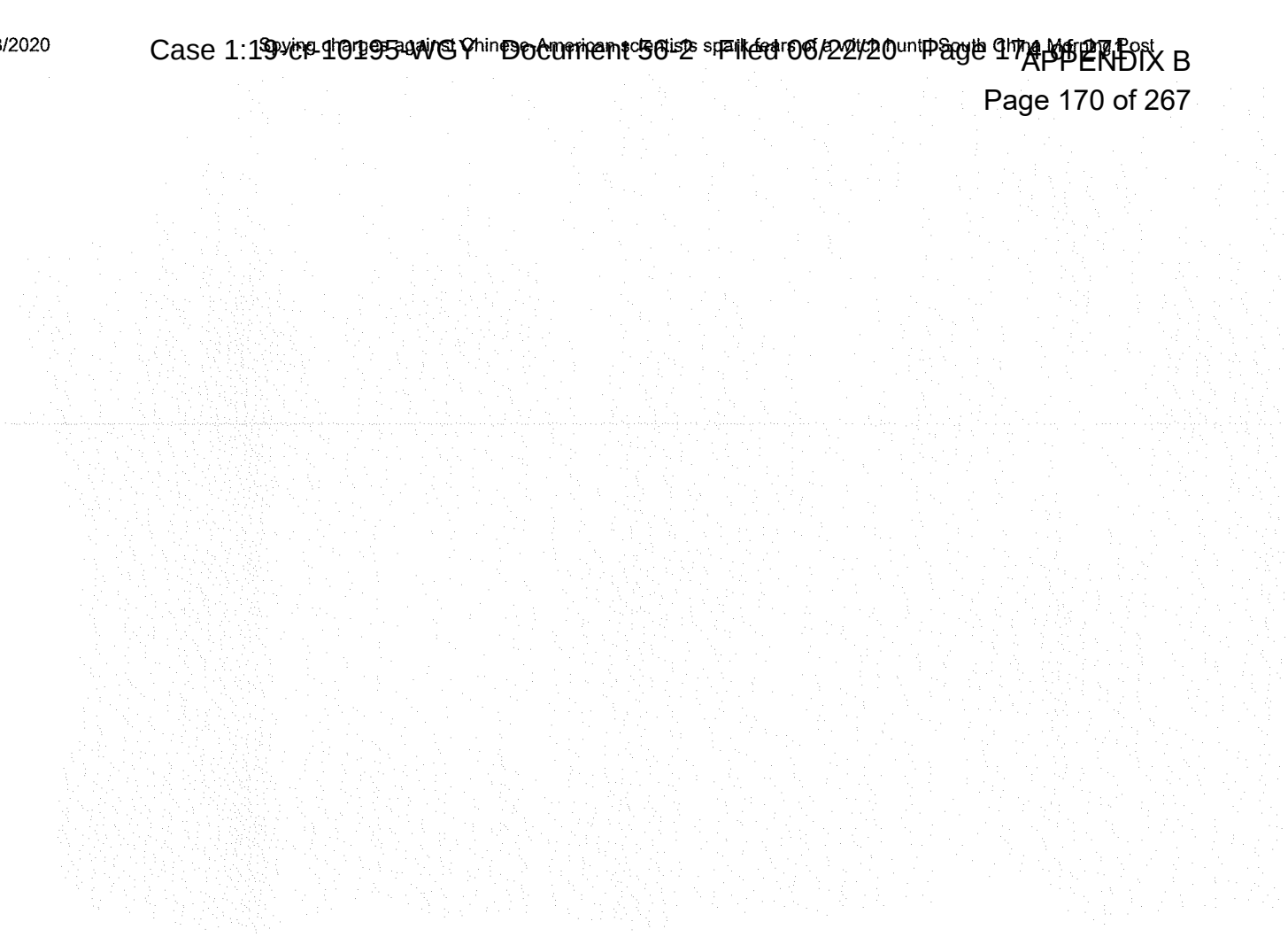
Rather than the pocket heater, say superconductivity researchers who reviewed emails and other case documents, Xi discussed two distinct magnesium diboride heaters – one that he invented himself and the other based on his invention – that are fundamentally different from the STI device. The labs he offered to help establish, meanwhile, would have focused on an entirely different line of research (oxide thin films), and thus would not have involved research with the pocket heater or another magnesium diboride heater.

The investigation's premise is off-base, according to Larbalestier. "The whole idea that there are huge pots of money that anybody is making out of magnesium diboride is just wrong," he says. The compound, Larbalestier adds, is still in development as a superconducting material, and commercialisation is "a decade or two decades away".

And as John Rowell, a research professor at Arizona State University, Tempe, wrote in an affidavit, the STI pocket heater, itself a modification of an existing technology invented in Germany in 1993, "is in no sense a revolutionary device".

Others say the case was based on a misreading of the scientific partnerships and teaching exchanges that have flowered since China began aggressively investing in research in the 1990s. Xi's offer to help Chinese colleagues build a world-class lab is a common gesture in international collaborations on superconductivity, which is highly developed in China, Chu says. "Ninety per cent of scientists involved in this kind of international exchange", he adds, could fit the description of Xi's activities in China.

"I am mystified as to why the case was brought," Larbalestier says.



Nuclear scientist Wen Ho Lee following his release from nine months of solitary confinement, in September 2000, in New Mexico. Picture: AFP

Critics of the US Justice Department's prosecutions say the government risks repeating the mistakes made in the case against Wen Ho Lee, who was charged with stealing secrets connected to the US nuclear arsenal in 1999. The Taiwanese-born physicist spent nine months in solitary confinement as the case against him deteriorated. Though he engaged in suspicious behaviour while at the Los Alamos National Laboratory, and ultimately pleaded guilty to one felony count of mishandling secrets, the government was never able to prove that he had conducted espionage.

James Parker, the judge in the case, apologised to Lee for the "demeaning, unnecessarily punitive conditions" in which he was detained and denounced cabinet officials for having "embarrassed our entire nation and each of us who is a citizen of it".

"Yes, America has a legitimate concern about cyber hacking and trade secrets theft," says Brian Sun, a trial lawyer with law firm Jones Day in Los Angeles, California, who represented Lee in a successful civil suit against the government. "But [...] do your homework. Get the science right before you put these people through the wringer."

America's hidden role in Chinese weapons research

Although the charges were dismissed, Xi says that finding himself in the government's cross hairs damaged his career. Before his tribulations began, he had been asked to co-author a chapter for a prestigious handbook on superconductors. After the news broke, he says, several co-authors threatened to pull out if he was kept on the project. Although his team continued its research, with other scientists assuming the principal-investigator roles he had held, the lab lost critical time on projects funded by grants due for renewal. Eventually, Xi says, his department arranged for him to talk to senior colleagues via teleconferencing, but because he was forbidden to talk to potential witnesses, he did not communicate with his students.

Adrift at home for four months, he devoted much of his time to his case.

The string of cases has Chinese-American scientists scrambling to understand how they might avoid being targeted. The Committee of 100 – a group of influential Chinese Americans whose members include former Nasa astronaut Leroy Chiao and David Ho, scientific director of the Aaron Diamond Aids Research Center in New York – has held seminars across the country for scientists outlining laws governing theft of trade secrets and export controls on critical technologies and explaining how to avoid inviting suspicion.

My reputation obviously has been damaged by this. If this happened to somebody else, I would

think that they probably did do some little thing wrong, at least
Xiaoxing Xi

Scientists involved in collaborations with China or Chinese colleagues "need to assume that their communications are being scrutinised" and "be clear and precise about what they're communicating", Zeidenberg cautions. "There's an assumption that any collaboration is suspect and potentially problematic."

"We need a set of well-defined rules," says Albert Chang, a physicist at Duke University, in North Carolina, and the president of the International Organisation of Chinese Physicists and Astronomers. "The indictments have instilled a great deal of uncertainty and anxiety in our community. People are wondering, 'Is this going to happen to me?'"

The Committee of 100 and others are pressing the government for more clarity.

Last year, Xi fielded a complaint against Haugen, the FBI agent who handled his case. He alleged that Haugen, along with officials at the FBI, National Security Agency and DOJ, violated his constitutional rights by having "intentionally, knowingly, and recklessly provided federal prosecutors with false scientific opinions" about his collaborations with labs in China. The behaviour was "extreme and outrageous" and led to press reports falsely portraying him as a spy, the suit continues, adding that in the raid on his house, Xi was treated like "an armed, dangerous terrorist".

"One of Professor Xi's greatest concerns," says Jonathan Feinberg, one of the lawyers representing Xi in the complaint, "is making the point that academic collaborations are not for a sinister and unlawful purpose."

Professor charged with industrial espionage in US says it discriminates against Chinese scholars

Xi now tours the US to speak about his case. He has resumed his work at Temple University, but he worries about obtaining research funding, regaining colleagues' trust and attracting collaborators.

"My reputation obviously has been damaged by this," he says. "If this happened to somebody else, I would think that they probably did do some little thing wrong, at least."

The ordeal has made him apprehensive about even the most basic of interactions.

"I was charged for things that were just normal collaborations," Xi says. "If all these normal activities could be seen as criminal activities, then the environment is quite frightening."

An earlier version of this story appeared in Science Magazine

Source URL: https://scmp.com/magazines/post-magazine/long-reads/article/2144652/spying-charges-against-chinese-american

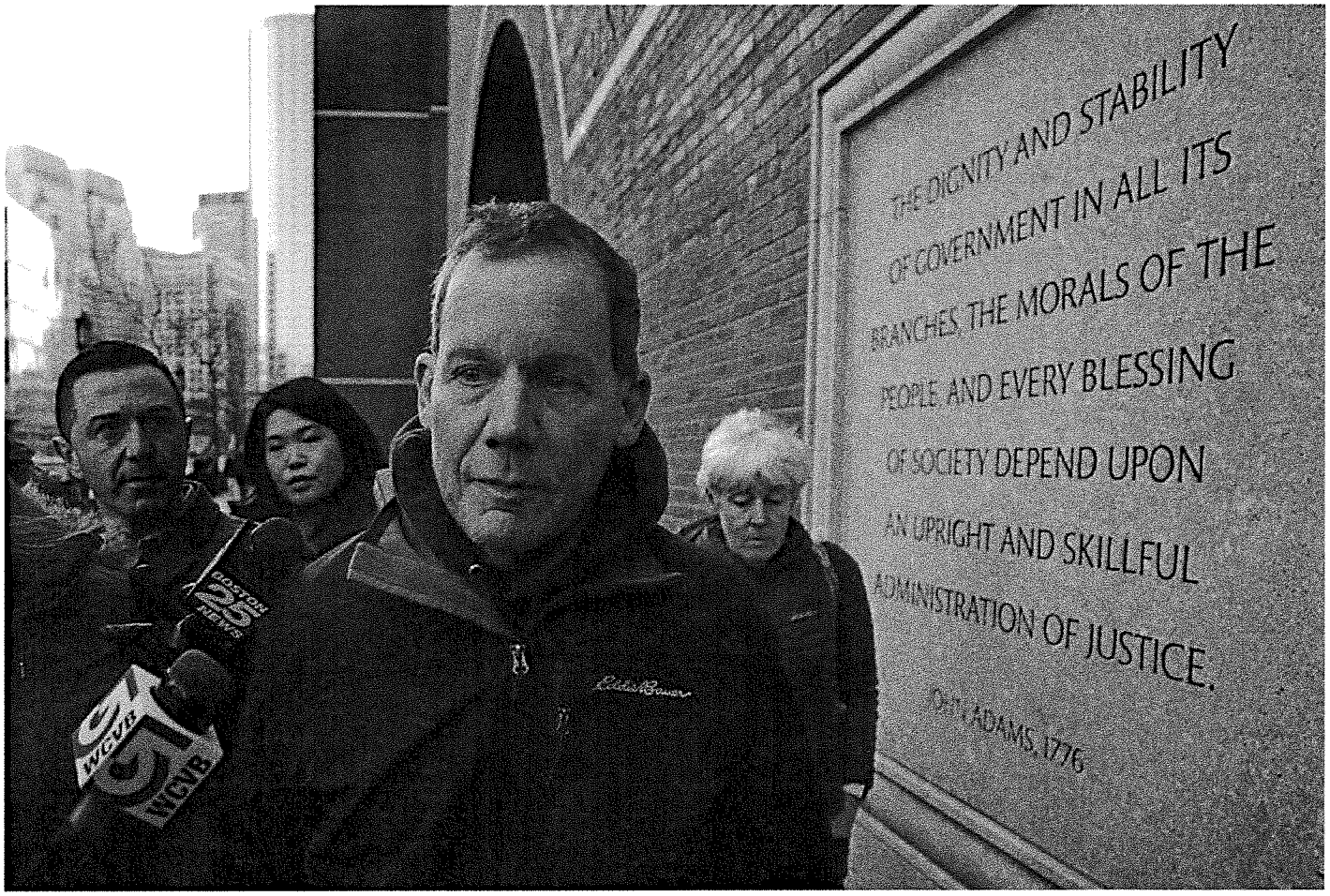
Links
[1] https://www.scmp.com/news/world/article/1858650/chinese-american-scientists-reveal-agony-being-accused-us-passing-secrets
[2] https://www.scmp.com/news/world/article/1807870/temple-university-professor-charged-offering-sensitive-data-china
[3] https://www.scmp.com/comment/insight-opinion/article/1860620/leaders-and-china-and-us-must-set-clear-rules-espionage
[4] https://www.scmp.com/news/china/article/1441827/us-convicts-two-selling-dupont-trade-secrets-chinese-state-owned-firms
[5] https://www.scmp.com/news/world/united-states-canada/article/2093876/chinese-born-professor-sues-fbi-agent-over-arrest
[6] https://www.scmp.com/news/china/diplomacy-defence/article/2082738/americas-hidden-role-chinese-weapons-research
[7] https://www.scmp.com/magazines/post-magazine/long-reads/article/2114110/chinese-american-astronaut-how-his-space-dream
[8] https://www.scmp.com/news/china/diplomacy-defence/article/1866890/professor-charged-industrial-espionage-us-says-it

OPINION

The intel on China's counterintelligence threat to America

China's assault on US technological know-how is so pervasive that in 2018 the attorney general formed the "China Initiative" specifically to combat the problem.

By **Andrew Lelling and Joseph Bonavolonta** Updated February 11, 2020, 3:50 a.m.



Harvard University professor Charles Lieber leaves the Moakley Federal Courthouse in January with his wife Jennifer, right, in Boston. Lieber, chair of the department of chemistry and chemical biology, was charged with lying to officials about his involvement with a Chinese government-run recruitment program through which he received tens of thousands of dollars. CHARLES KRUPA/ASSOCIATED PRESS

The ruling Communist Party of the People's Republic of China is engaged in an

unprecedented long-term campaign of espionage and intelligence collection against American businesses, universities, research facilities, and other sensitive locations. There is nothing speculative about this concern. Eighty percent of federal prosecutions for economic espionage allege direct involvement of the Chinese government. About 60 percent of all prosecutions for economic espionage have at least some connection to China. Chinese theft of research and technology costs our country between $225 billion and $600 billion a year. As FBI Director Christopher Wray recently told Congress, "There is no country that poses a more severe counterintelligence threat to this country right now than China."

We in New England have been directly harmed by this aggressive campaign. For example, American Superconductor Corporation, a wind energy company based in Devens, lost over 700 jobs and more than $1 billion in shareholder equity when a Chinese company, Sinovel, stole proprietary software used in wind turbines. Sinovel was eventually convicted on federal criminal charges, but that was small consolation in light of the layoffs and drop in share value due to lost technology.

American Superconductor is not an outlier. In 2018, federal prosecutors in Boston charged a Chinese national with conspiring to illegally export sonar buoy technology — used to track submarines — to a Chinese entity linked to the People's Liberation Army. In December 2019, a Chinese national, Zaosong Zheng, was charged with stealing biological agents from the Beth Israel Deaconess Medical Center and trying to smuggle them to China.

Our universities are at risk as well. In late January, Harvard professor Charles Lieber was charged with lying to federal authorities about his involvement in a Chinese talent-recruitment program, Thousand Talents. Lieber, whom the Chinese allegedly paid a whopping $50,000 a month, is a world-renowned researcher in nanotechnology. Boston federal prosecutors also recently charged a university researcher with omitting on her immigration paperwork that she is a lieutenant in the People's Liberation Army.

Make no mistake: China is trying to fill its strategic gaps at the expense of other nations. As outlined in its own Made in China 2025 initiative and most recent Five-Year Plan, China is striving for self-sufficiency in key research and technical sectors, and it is doing so by stealing technology from foreign countries, replicating it for domestic use, and then replacing the original, foreign tech with its own, first in the domestic market and then globally.

Beyond the cases described above, in the last six months the FBI and the Justice Department have investigated and charged similar conduct by Chinese nationals in Arizona, California, Florida, Illinois, Missouri, Ohio, Tennessee, and elsewhere. The FBI is now investigating China-related cases in all 50 states, encompassing all 56 FBI field offices.

China's assault on US technological know-how is so pervasive that in November 2018 the attorney general formed the China Initiative specifically to combat the problem. The Boston US attorney is one of the five steering committee members for the initiative, which has provided guidance to US attorneys nationwide on prioritizing aggressive, innovative prosecutorial strategies for countering this threat.

We rightly celebrate the culture of openness in US academia, and foreign visitors who study, innovate, and start businesses here make our country stronger. We know that most Chinese students and researchers in the United States are here for legitimate academic purposes. But some are not. The Chinese government routinely recruits some percentage of Chinese nationals and others to assist in intellectual property theft.

China takes a broad approach to these efforts, using not just intelligence officers but academics, businesspeople, students, and other civilians to achieve its strategic objectives. We must likewise embrace a holistic approach to countering the threat. Federal authorities routinely develop partnerships with private institutions to enhance awareness, and we all share the goal of confronting this problem while maintaining a

welcoming atmosphere for foreign researchers. Universities and businesses should urge transparency in dealings with foreign entities, including the Chinese government. Federal agents and prosecutors cannot do the job alone.

Andrew Lelling is the US attorney for Massachusetts. Joseph Bonavolonta is the special-agent-in-charge of the FBI's Boston field office.

Show 16 comments

©2020 Boston Globe Media Partners, LLC

THINKING ABOUT THE HORIZON

THE NEXT 20

Just the Wrong Amount of American

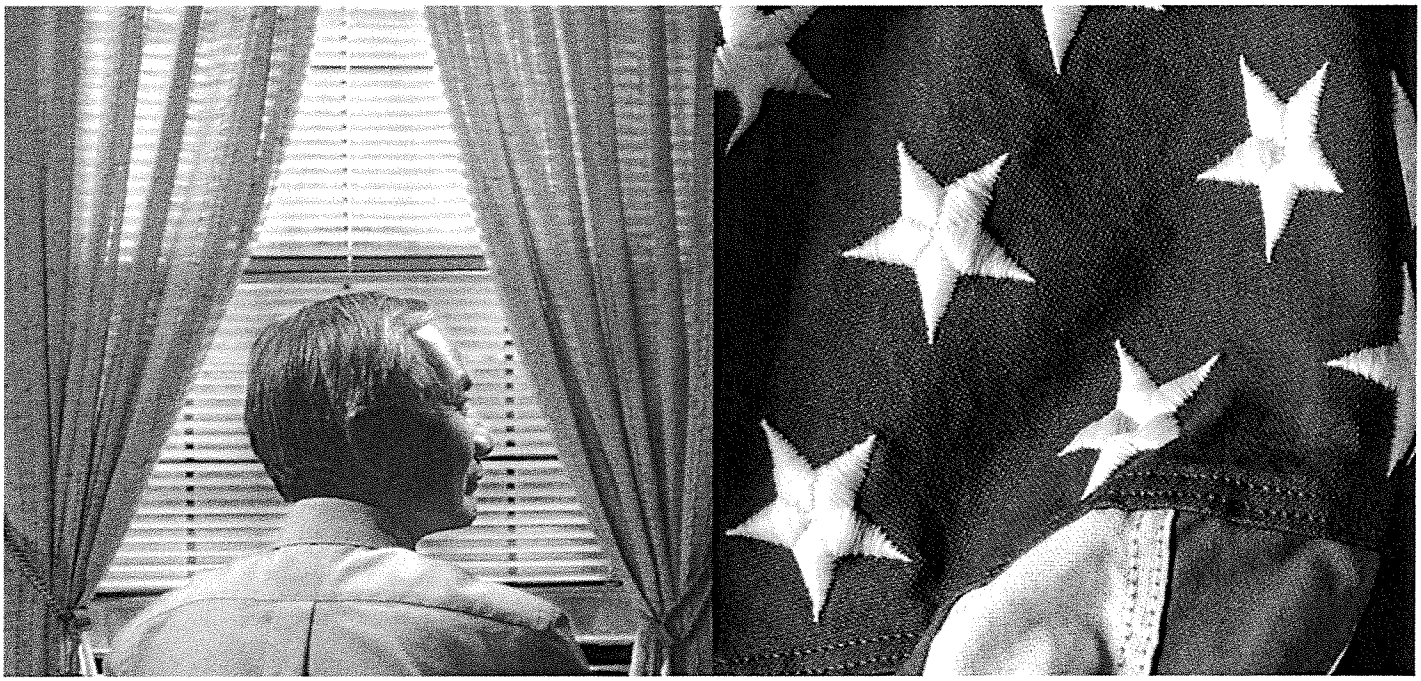
Wen Ho Lee's 1999 arrest taught Chinese Americans that their country may never trust them.

By LOWEN LIU
SEPT 11, 2016 • 9:20 PM

TWEET

SHARE

COMMENT



Wen Ho Lee, who in 1999 was accused by the U.S. Justice Department of being a Chinese spy, on Dec. 15, 2000, in his Los Alamos, New Mexico, home.

Photo illustration by ***Slate***. Photos by Thomas Michael Alleman/Liaison/Getty Images and iStock.

On March 6, 1999, the *New York Times* published an explosive report by James Risen and Jeff Gerth that a spy at Los Alamos National Laboratory had given U.S. nuclear secrets to China, including the design of the most advanced American warhead, the W-88. The story reverberated in the halls of the Capitol, where Republican leaders had long been trying to pin the Clinton administration for ignoring the dawn of a new cold war. The unnamed spy was described as "Chinese-American."

Two days later, before any arrest or charges had been made, the *Times* identified the suspect as Wen Ho Lee, a Taiwan-born scientist, and reported he'd just been fired from the lab. The original story had forced the FBI into a rushed interrogation of Lee, in which an agent threatened Lee by comparing him to the Rosenbergs; Secretary of Energy Bill Richardson, desperate to prove his department was not as hapless as it seemed, directed that Lee be fired without review. Intelligence official Notra Trulock, a central figure in the original *Times* story, would later say that it was Richardson who had leaked Lee's name to the press. Lee was the only suspect under investigation.

In the months that followed, no charges were brought. Dozens of agents descended on Los Alamos, New Mexico, to prove what had become accepted fact in Congress and in the public eye: that Wen Ho Lee had betrayed the country he was a naturalized citizen of, and in the worst possible way. He'd given China the keys to the destruction of the United States. When in December Lee was finally arrested, he was charged not with nuclear espionage, for which there was no evidence, but with 59 counts of downloading restricted data to unrestricted systems. Prosecutors told the court that the knowledge Lee possessed threatened the safety of every single American, and he was placed—before trial—into 23-hour-a-day solitary confinement, shackled for his one hour of exercise. To prevent him from passing secrets, he was forbidden to speak in Mandarin during family visits.

Nine months later, in September 2000, Lee pleaded guilty to one felony count of mishandling data and was released. Thus ended, at least officially, the 18-month fiasco that exposed an American security apparatus as both too vulnerable to political influence and too unchecked in its investigative and prosecutorial abilities, all in the name of the national interest.

It can be easy to forget the enormity of the Wen Ho Lee debacle. Nearly every assumption the government made—that China had acquired a miniature-warhead design through espionage, that Los Alamos had been its source, and that it had done so using intel from a "master spy"—was refuted by the facts. After Lee's release, the *New York Times* conducted an internal investigation, detailing what "we wish we had done differently" in its one-sided and sensationalist stories but retaining a defiant tone that disappointed critics who believed the paper had stoked the entire ordeal. (In 2006, Lee would receive a settlement from the government and several newspapers including the *Times* for the leaking of his name.) The federal judge, in releasing Lee, offered an extraordinary and emotional apology, firing a salvo at the executive branch for drumming up the case and causing "embarrassment to our entire nation and each of us who is a citizen in it."

As purely a story of government overreach and journalistic malpractice, the Wen Ho Lee case is worth revisiting. But as China, a nation the U.S. courts and distrusts in equal measure, looms ever larger on the world stage, Chinese espionage cases have been on the rise—many of them eerily reminiscent of Lee's. Suspects are branded as traitors, with the might of the government arrayed against them, because they are Chinese. It's become clear that despite the embarrassment the Lee case brought to multiple branches of government, it was not the closing chapter to an ugly period of suspicion and prejudice—it was the beginning.

Guoqing Cao and Shuyu Li, scientists at Eli Lilly, were arrested in October 2013 for passing $55 million worth of secrets to a Chinese drug company. They were jailed and then placed under house arrest; the charges were changed to wire fraud and then dropped in December 2014. The proprietary information they passed was not proprietary after all.

Sherry Chen, a hydrologist at the National Weather Service, sent publicly available info to an old classmate in China and referred that person to a colleague for further information. The colleague reported her as a potential spy, and she was arrested in October 2014. Charges were dropped in March 2015, but the National Weather Service has refused to give Chen her job back.

Xiaoxing Xi, then chair of the Temple University physics department, was arrested in May 2015 for sending plans to a device used in semiconductor research, known as a "pocket heater," to China. The plans were not of a pocket heater; investigators without the proper scientific background had mixed them up. The charges were dropped in September of last year.

Other similar cases are on the way to trial. The espionage suspicions these days often center on corporate secrets, rather than government ones, but the course of the cases is familiar: sudden arrests and long investigations during which any minor slip-up—even forgetting a date during an interrogation, as happened to Sherry Chen—becomes a lie that proves the crime. In the months or years that it takes to exonerate a suspect, lives are ruined. George Koo, a business consultant and member of the influential Chinese American advocacy group the Committee of 100, described this to

me as the government's "first-move advantage," one that distorts the justice process. Given the power, resources, and secrecy involved in espionage prosecutions, the burden of proof nearly always ends up with the defense.

Other recent suspects of Chinese ethnicity, it should be said, have been found guilty. The theft of industrial and trade secrets has been referred to as the single largest loss of American wealth, guesstimated in the hundreds of billions of dollars a year. The FBI has long held that China is unique in its intelligence-gathering methods, that instead of relying on trained operatives, it accumulates as much information as it can, in bits and pieces, from anywhere—public sources, overseas students, scientists visiting China, and, yes, by appealing to the sympathies of Chinese Americans. A version of this theory can be found in *A Convenient Spy*, the fair and deeply reported 2002 book on the Lee case by Dan Stober and Ian Hoffman. Former FBI chief of Chinese counterintelligence Paul Moore describes the Chinese approach as "grains of sand," in which the recruitment pitch is made to as many targets as possible and begins simply, "Are you a friend of China?" Moore has argued that since China's strategy targets more ethnic Chinese by number than non-Chinese, racial profiling in U.S. counterintelligence is unavoidable.

ADVERTISEMENT

You May Like

Sponsored Links by Taboola

Which Travel Card Has The Most Valuable Miles?

NerdWallet

FDA Approved KN-95 Masks Available [Buy Here]

Stratton Medical Supply

The Most Beautiful Sideline Reporters Ever

Sportinal

It's unclear whether profiling plays an official or simply tacit role in the FBI's counterintelligence strategy. On a 2004 *Frontline* feature about Chinese spying, former FBI agent Edward Appel said that using "a different lens" for anyone with Chinese ancestry "isn't a double standard when you stop and think about it. ... It's basic counterintelligence methodology and security methodology." What defenders of a "different lens" miss, however, is that even if China recruits more ethnic Chinese spies (but not exclusively), profiling is not just wrong morally; it's foolish. The presumption of guilt leads to sloppy investigations: Technical specifications are not examined closely; benign explanations are bypassed; other suspects are ignored. It leads to cases like Wen Ho Lee's.

When the Department of Energy opened its operation to hunt for the supposed W-88 spy in the mid-'90s, investigator Dan Bruno penned a memo that said, "An initial consideration will be to identify those US citizens, of

Chinese heritage, who worked directly or peripherally with the design development"—race as a factor to whittle the field. A (rejected) FISA surveillance application by the FBI explicitly listed "ethnic Chinese" among its reasons for tapping Lee's phone. Lee had visited China in the '80s (for the first time in his life), filling one of the DOE's criteria, but so had many other non-Chinese scientists from the national labs who were never investigated. Notra Trulock, the DOE intelligence officer, provided star testimony for the House's doomsday Cox Report, declassified two months after Lee was named, which suggested that every person of Chinese ancestry was a potential sleeper agent for the United States' greatest rival. For years, the Cox Report would become shorthand in the government for the threat of China, even after its most alarmist findings were thoroughly debunked.

That's not to say Lee never behaved suspiciously. He'd been investigated once in the early 1980s for cold-calling a Taiwan-born scientist who was under surveillance (eventually assisting the FBI in an intelligence operation around that scientist), and then again in the late '90s for having failed to report an earlier, brief encounter with a Chinese nuclear-weapons official. Then there was the downloading of data for which he ultimately pleaded guilty—but these codes, nuclear-weapons experts said, were so tailored to American testing and engineering that they could not possibly have been intended for or useful to China. In their book, Stober and Hoffman reasonably surmise that the inconsistencies and deceptions revealed in the investigation of Lee likely came from a deep sense of inadequacy, not intrigue. Lee was an unspectacular scientist (as far as nuclear scientists go),

worried about his job security and eager to prove his worth. Former Los Alamos counterintelligence chief Robert Vrooman found Lee to be naïve and thus vulnerable, but not a spy. Countering the FBI's ethnicity-focused approach, he wrote: "It was our experience that Chinese intelligence officials contacted everyone from the laboratories with a nuclear weapons background who visited China for information, regardless of their ethnicity."

But this is the power of racial profiling, to elevate suspicious behavior to prosecutable crime. That Lee's case had some ambiguity makes it a more valuable example, not less. After all, who, given enough scrutiny, is not suspicious? Put simply: It was a bad case, with a suspect who didn't fit the charge in any way but one—and yet that one dimension was convincing enough that a GOP Congress, the FBI, and the Departments of Energy and Justice, with an assist from the media, all stopped squabbling long enough to agree that Lee should be put away as a traitor.

* * *

The Lee case was also the biggest test of a newly mature Chinese American movement. And at first, the community's response was tentative and fragmented. Modern Chinese America is young; immigration was banned or heavily restricted between the Chinese Exclusion Act of 1882 and the Immigration and Nationality Act of 1965. The emergent movement found a national voice in 1982, after Chinese American Vincent Chin was beaten to

death by two Detroit autoworkers who blamed the industry's decline on Japan.

But the Wen Ho Lee case was a different challenge. When the *Times* published its March 6 story, a collective seizure went through the Chinese American community, which worried it would have to choose between defending one man's right to due process and giving him up to protect the rest of the community from fallout discrimination. "I called a meeting of 15 Asian American rights organizations in San Jose," said Ling-chi Wang, a founder of the San Francisco–based Chinese for Affirmative Action, "and presented a two-page plan" for how to collectively approach the Lee case. No one bit.

At the outset, the Committee of 100 had taken an approach of comity. It invited Bill Richardson to speak at its convention in April 1999, where he reassured them that "Americans are Americans." By the spring of 2000, when it was clear Lee was being railroaded, Wang advocated for a boycott of government laboratories by Chinese American scientists. Many scientists responded with anger at Wang for making their lives harder than they'd already been since Lee became the face of Chinese treachery. A prominent member of the Committee of 100 initially called the effort "counterproductive." (The boycott would eventually be a success.)

"My first sense was this was not good for us, whether he was guilty or not," Albert Wang, founder of the Bay Area's Citizens for Better Community, told me. "We were nothing back then." He remembered that the national headquarters of the largest advocacy group, the Organization for Chinese Americans (now known as Asian Pacific American Advocates) initially refused to offer support. What if Lee was guilty? It was too big a risk.

This is the divided consciousness that afflicts those singled out for their race. I was 21 and not all that politically minded when the *Times* report came out. My first thought was along the lines of "That rat!"—and it seemed the best way I could prove my patriotism and honor my kind, even privately, was to hope the spy was brought to justice, definitively and swiftly.

A childhood friend of mine, Roger Hu, then at MIT, did get involved with the movement after Lee was arrested. He helped run a website for Lee's legal defense fund. When MIT's Chinese Students Association declined to support the cause, he walked down Massachusetts Avenue to ask Harvard's. Speaking out was brave and necessary. I feel some shame and regret now that I did not say anything then, that I believed it was more proper and prudent not to. Even when Lee was released, I was ambivalent, skeptical of the man even as I understood that all Chinese Americans would suffer for the injustice that had been done to him. Roger invited me to a party celebrating Lee's release, in December 2000, where I shook Lee's hand and didn't know exactly what to feel. Now I do.

What makes a movement? Albert Wang told me it is a "numbers game"—in terms of the U.S. population, where Asians are the fastest-growing racial demographic, but also in our government, which historically has not been high on the list of careers considered by Asian immigrants and their children. There are currently 10 U.S. representatives of Asian descent, less than half of what would give Asians representation proportional to their population. (At the time of Wen Ho Lee's arrest, there were only three.) But it's not just numbers; it's also about voice. Many felt it was better to remain silent during the Wen Ho Lee case not only because of ambivalence about his guilt, but because we didn't see or didn't want to see the through lines of racism that touched us all. There's little excuse now.

Pollsters remain puzzled why Asians, the wealthiest racial demographic, still vote to the left, and social scientists breezily wonder out loud if it won't be long before whiteness invites Asians to join the club. I'm doubtful. As long as Asians continue to be reminded they ultimately do not have say over their own Americanness, they will have more in common with the other minority groups vulnerable to the caprice of public fear and political fearmongering. Muslims and Arabs are terrorists; Latinos are undocumented job-thieves; blacks are violent criminals. And Chinese—those circumspect, duplicitous, sneaky Chinese—are spies.

There is a reckoning coming for people of color, as the steady march toward a majority-minority country butts up against retrenched white nationalism, currently feeding on the legitimacy of Donald Trump's campaign. For Chinese Americans, the contours of how that reckoning might take place are visible thanks to Wen Ho Lee. Referring to trade deficits, Trump has said, "We can't continue to allow China to rape our country." His website includes zero-tolerance language about "China's ongoing theft of intellectual property." It's not hard to imagine Trump, or whoever comes after him, drastically affecting Sino-American relations; and thus the lives of Chinese Americans.

Wariness is now the word. The next generation of Chinese American voices will have to remember that despite their patriotism, their relative privilege, their country doesn't trust them. This is the enduring lesson of Wen Ho Lee, the Patient Zero of the unnerving present and uncertain future of being Chinese in America. He was there at the wrong time, had made just the wrong amount of missteps, and was just the wrong amount of American. After Lee's release, activists pushed for him to receive a presidential pardon, but it never came. He published a textbook and a memoir and, unable to find another job, retired in New Mexico. Lee doesn't appear to have given an interview in over a decade, and I wasn't able to reach him, so it's not clear what he thinks these days, about his brief reign as spy of the century or about the conduct of justice in his adopted country. But I do take heart in one detail that has remained true since he regained his freedom: He's still here.

Tweet Share Comment

Next 20

YOU MAY LIKE

Which Travel Card Has The Most Valuable Miles?
NERDWALLET | SPONSORED

FDA Approved KN-95 Masks Available [Buy Here]
STRATTON MEDICAL SUPPLY | SPONSORED

The Most Beautiful Sideline Reporters Ever
SPORTINAL | SPONSORED

MOST RECENT

People Like Amy Cooper Are Why I Left New York City
AYMANN ISMAIL

Trump Retweets Interview Trashing George Floyd's Character as He Breaks Own Twitter Record
DANIEL POLITI

Crying Wolf on Kushner SLATE STAFF

Trump Can't Heal America SLATE STAFF

The Inconceivable Strangeness of Trump's Bible Photo-Op
RUTH GRAHAM

My Family Is the Only One in the Neighborhood Still Social Distancing
JAMILAH LEMIEUX

NerdWallet | Sponsored
Which credit card has the best travel rewards? See the list.

Stratton Medical Supply | Sponsored
Buy 2 Boxes Get 1 Free: Disposable Face Masks

Penguin M.D. | Sponsored
The Women That Tiger Woods Betrayed His Wife With

NerdWallet | Sponsored

High-interest savings accounts that earn you piles of cash

CBS News | Sponsored

We Ranked Every Oscar Best Picture Winner From Worst To Best

Quicken Loans | Sponsored

Quicken Loans Is Making Refinancing As Simple As Possible

Online Stores LLC | Sponsored

50 Disposable Masks $26.95, 100 Gloves $8.95

Kiera Store | Sponsored

Brilliant New N95 Sports Masks Sweeping US

Fresh Edits | Sponsored

'Flip or Flop' Contractor Led to El Moussa's Divorce

PensAndPatron | Sponsored

Jessica Simpson Was The Prettiest Cheerleader At Her High School

Bill Cruncher | Sponsored

Massachusetts : Launches New Policy For Cars Used Less Than 59 Miles/Day

Space Masks | Sponsored

Premium Masks with 3 Nanotech Layers. Free Same Day Shipping. Get Yours

BrainSharper | Sponsored

She Made A Fortune From Commercials Alone

WearableAC | Sponsored

New Portable AC Flying Off Shelves in United States

EverydayKoala | Sponsored

Paige Spiranac's Mini Dress; Stir On Red Carpet

The Inconceivable Strangeness of Trump's Bible Photo-Op

Post Fun | Sponsored

These Twins Were Named "Most Beautiful In The World," Wait Till You See Them Today

Hunt A Killer | Sponsored

This "At-Home" Murder Mystery Will Keep You Busy for Hours

Stadium Talk | Sponsored

25 Worst MLB Hall of Famers, Ranked

Reprints
Advertise: Site / Podcasts
Commenting
Podcast FAQs
Contact / Feedback
Pitch guidelines
Corrections
About us

Work with us
Send us tips
User agreement
Privacy policy
AdChoices
Slate Shop
Do Not Sell My Personal Information

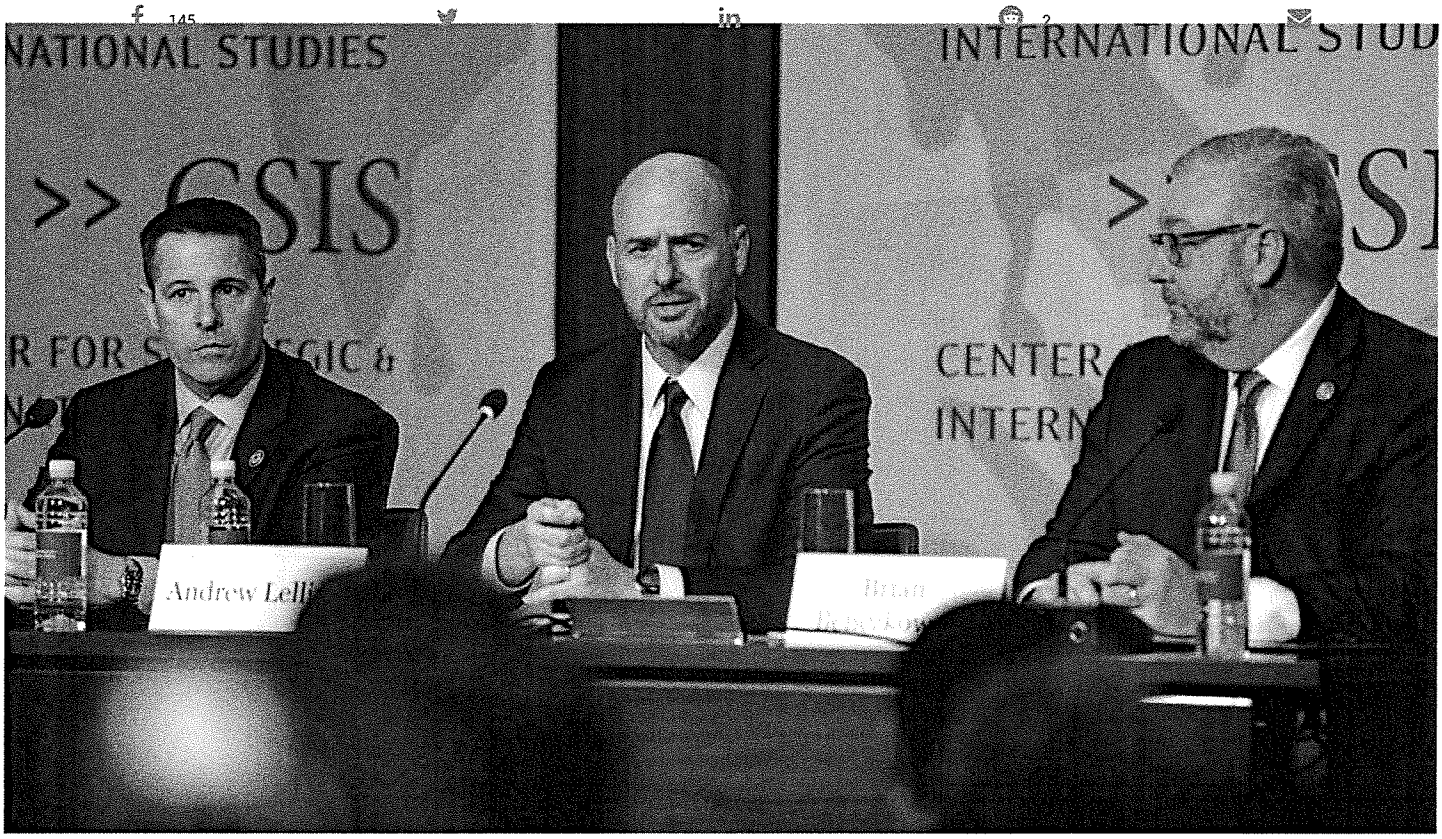
FOLLOW US
Facebook
Twitter
Instagram
RSS Feed

Slate is published by The Slate Group, a Graham Holdings Company.
All contents © 2020 The Slate Group LLC. All rights reserved.

Become a Member

Read our COVID-19 research and news.

Advertisement



Andrew Lelling, U.S. attorney for the district of Massachusetts, explains recent prosecutions under the Department of Justice's China Initiative at a 6 February event in Washington, D.C. To his left is Jay Town, U.S. attorney for the northern district of Alabama. CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

U.S. attorneys warn of upcoming 'spike' in prosecutions related to China ties

By **Catherine Matacic** | Feb. 7, 2020 , 3:15 PM

Researchers in academia and industry who work with Chinese institutions should expect a "spike" in prosecutions this year as a result of a U.S. government initiative to stop economic espionage, say federal prosecutors leading the effort. And although they say the criminal cases could harm potentially useful U.S. collaborations with China, the prosecutors believe they will help deter future problems.

"Some will complain that [the prosecutions] might have a chilling effect on collaboration with the Chinese. The answer to that is—for good and bad reasons—yes, it will," said Andrew Lelling, U.S. attorney for the district of Massachusetts, at an event yesterday in Washington, D.C. "China has launched a massive nationwide effort to pilfer U.S. technology and know-how and transfer it to China for its own uses, so unfortunately this kind of response is needed."

Lelling was just one panelist appearing before a packed house at the Center for Strategic and International Studies for an event featuring Attorney General William Barr and FBI Director Christopher Wray. The discussion, which included representatives from academia and industry, focused on the Department of Justice's (DOJ's) China Initiative, which aims to disrupt what U.S. officials say is a systematic effort by the Chinese government to obtain advanced technology with economic and military value.

SIGN UP FOR OUR DAILY NEWSLETTER
Get more great content like this delivered right to you!

Email Address *

The China Initiative, launched in November 2018 by then–Attorney General Jeff Sessions, has so far led to more than 40 arrests on an array of charges, according to **an FBI presentation** supported by **DOJ documents**. About 1000 investigations are open, Wray said, "in every industry and sector," including academia.

Those cases are starting to unsettle researchers who think, **often with good reason**, that espionage fears are overblown, said Mary Sue Coleman, president of the Association of American Universities, a group of top research universities in the United States and Canada. "When they see a department chair at Harvard being called to account and who may go to jail … that has done more to help us [convince them] than anything abstract that we could possibly have done," she said.

In response to the increased scrutiny of foreign collaborations, colleges and universities are ramping up efforts to educate faculty about potential threats, said Doug Girod, chancellor of the University of Kansas. They're also expanding efforts to monitor foreign travel, funding sources, and outside commitments, including part-time appointments in overseas schools and labs. Because the potential conflicts of interest—and commitment of time—are so varied, and because there hasn't been a single set of guidelines from law enforcement and funding agencies, mounting a response has been tough. "I may have everybody disclose everything," Girod said. "That doesn't mean that I know what to do with it."

Lelling said such education and disclosure efforts are just what government officials hope will deter future problems. "That's 80% of the battle," he said. "Maybe next time an academic does not lie about his connections to a Chinese program, or maybe next time an academic thinks twice or thinks harder about collaborations with a Chinese institution and what the motivations of the institution might be."

Businesses have also been rattled. Recent high-profile cases linked to the initiative include those of an ex-Monsanto researcher charged with **stealing software to optimize crop output** and a scientist who **pled guilty** to stealing unnamed trade secrets from his former employer, Phillips 66. But when asked to appear on a panel at the event about economic espionage, multiple business executives declined.

"Why isn't a CEO up on stage with us today?" asked John Carlin, a former assistant attorney general for national security under the Obama administration, who organizers asked to fill in at the last minute. The U.S. government has plenty of sticks for prosecuting bad actors, he said, but "we lack the carrot" to convince most businesses to step forward publicly. The "fear of retaliation" is just too great, he said, whether in the form of lawsuits, Chinese government sanctions, or continued intellectual property theft.

Four U.S. attorneys tasked with leading the China Initiative, including Lelling, said to expect more outreach efforts—including a national conference later this year—and more prosecutions of both individuals and companies. In addition, Lelling said, prosecutors are coming up with "creative ways" to charge agents suspected of intimidating and monitoring Chinese nationals working and studying on U.S. campuses.

Though no representatives of the Chinese research or business communities were on stage, multiple speakers emphasized that the effort wasn't launched to single out or prosecute individuals of Chinese descent. "To be clear, this is not about the Chinese people as a whole, and it sure as heck is not about Chinese Americans as a group," Wray said. "But it is about the Chinese government and the Chinese Communist Party."

To clarify rules for researchers and businesses, the prosecutors said they would like to see the federal government settle on a single set of reporting guidelines from grantmaking bodies, including the National Institutes of Health, National Science Foundation, and the departments of energy and defense. They also floated a potentially controversial new requirement: having researchers with foreign collaborations register those arrangements with a single government body, much as lobbyists who work for overseas governments have to register as "foreign agents." Such a change, said Jay Town, U.S. attorney for the northern district of Alabama, would "give some real teeth" to prosecutors' efforts.

Coleman said the federal government's concerns about Chinese actions are warranted, but warned that equal efforts should be made to maintain the open and competitive nature of scientific collaboration that has given the United States a "powerful" advantage since the 1950s. "Kudos to the federal government for bringing these groups together to help us really know what the threat is, [and] develop the armor to protect ourselves from the threat, but not kill what has made us so powerful for the past 75 years."

Posted in: **Asia/Pacific**, **Science and Policy**
doi:10.1126/science.abb2156

Catherine Matacic
Catherine Matacic is an associate online editor, specializing in linguistics and the social sciences.
Twitter

More from News

Europe bets R&D spending will bring jobs to battered economy

Science's extensive COVID-19 coverage is free to all readers. To support our nonprofit science journalism, please **make a tax-deductible gift today.**

Got a tip?

How to contact the news team

Advertisement

Advertisement

Latest News

Trending

1. **A mysterious company's coronavirus papers in top medical journals may be unraveling**
2. **Blood vessel attack could trigger coronavirus' fatal 'second phase'**
3. **Why coronavirus hits men harder: sex hormones offer clues**
4. **Urban foxes may be self-domesticating in our midst**

2. **Study that claims white police no more likely to shoot minorities draws fire**

3. **Why do some COVID-19 patients infect many others, whereas most don't spread the virus at all?**

4. **Operation Warp Speed selects billionaire scientist's COVID-19 vaccine for monkey tests**

5. **Blood vessel attack could trigger coronavirus' fatal 'second phase'**

Sifter

Earth's species disappearing at an alarming rate
By Amanda Heidt | Jun. 4, 2020

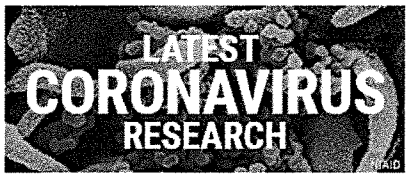
Watch an example of chimpanzee 'culture,' as one fishes for termites
By Amanda Heidt | May. 28, 2020

Our Moon is not as 'dry' as we thought
By Amanda Heidt | May. 8, 2020

Herpes virus can trigger Alzheimer's, brain tissue study suggests
By Kelly Servick | May. 7, 2020

Cancer drug dampens intrusive thoughts in men with pedophilic disorder
By Amanda Heidt | May. 1, 2020

More Sifter



Read the Latest Issue of *Science*

5 June 2020

Vol 368, Issue 6495

Table of Contents

ASTRONOMY
Double trouble

SCIENTIFIC COMMUNITY
Bill would supersize NSF's budget—and role

EUROPEAN NEWS
Europe bets R&D spending will bring jobs to battered economy

SCIENTIFIC COMMUNITY
Shuttered natural history museums fight for survival

MEDICINE/DISEASES
The pandemic's first major research scandal erupts

MEDICINE/DISEASES
Blood vessel injury may spur disease's fatal second phase

Get Our E-Alerts

- [x] First Release Notification
- [x] *Science* Careers Job Seeker

United States

Email address*

- [ ] I also wish to receive emails from AAAS/*Science* and *Science* advertisers, including information on products, services, and special offers which may include but are not limited to news, career information, & upcoming events.

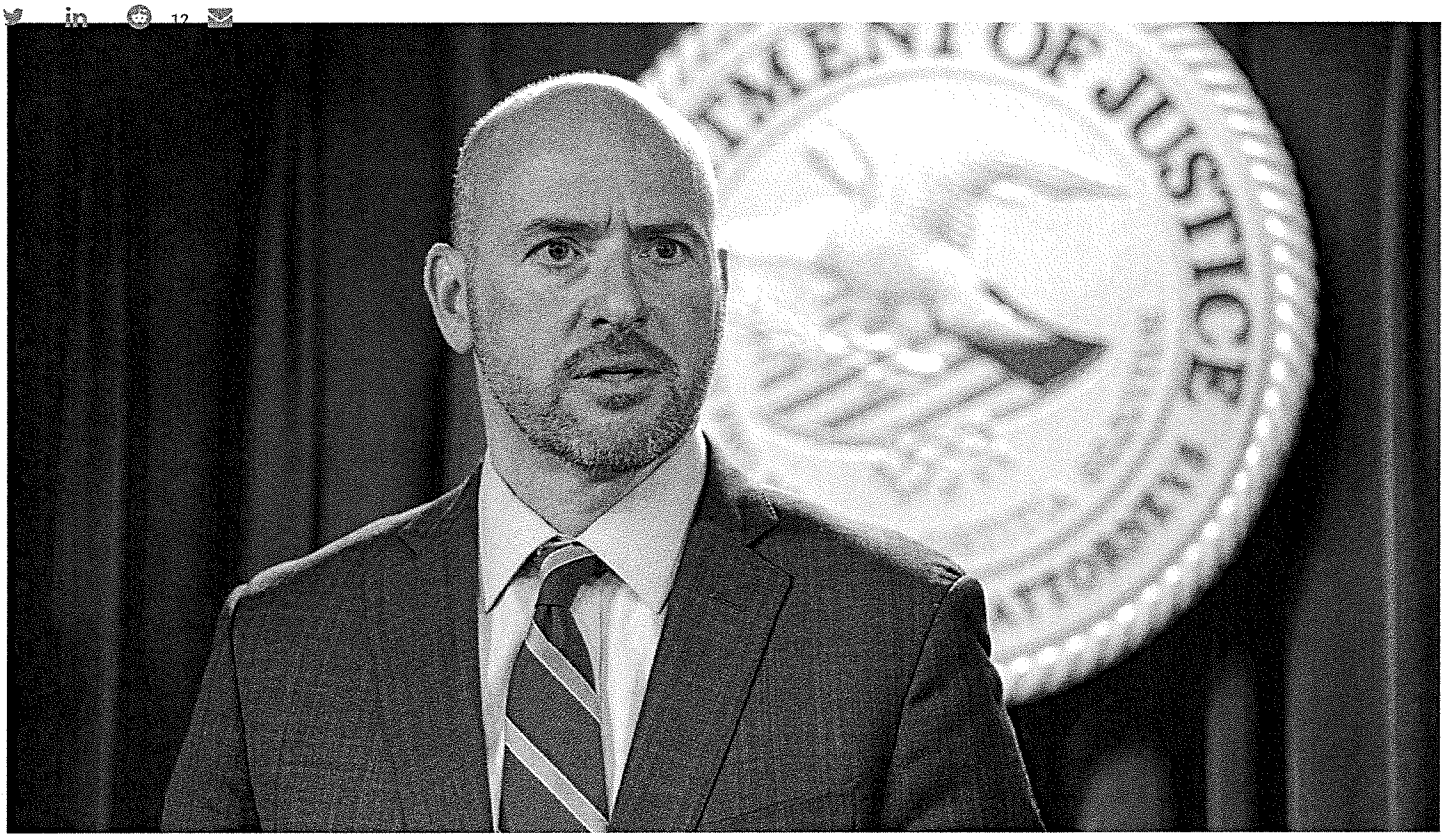
Sign up today

Required fields are indicated by an asterisk (*)

© 2020 American Association for the Advancement of Science. All rights Reserved. AAAS is a partner of HINARI, AGORA, OARE, CHORUS, CLOCKSS, CrossRef and COUNTER

Read our COVID-19 research and news.

Advertisement



Andrew Lelling KATHERINE TAYLOR/REUTERS/NEWSCOM

U.S. prosecutor leading China probe explains effort that led to charges against Harvard chemist

By **Jeffrey Mervis** | Feb. 3, 2020 , 11:45 AM

The U.S. government isn't prosecuting Charles Lieber because he's a world-renowned inorganic chemist at Harvard University, says the U.S. attorney who last week drew headlines by **charging Lieber with making false statements about his ties to Chinese research institutions.** Nor does the Department of Justice (DOJ) think for 1 minute that Lieber is a spy.

What worries Andrew Lelling, U.S. attorney for the Massachusetts district, is that Lieber was allegedly paid to carry out research in China, which, combined with his failure to disclose those relationships, makes him potentially vulnerable to pressure from the Chinese government to do its bidding at some future point. "It was the amount of money involved that drew our attention," Lelling says, referring to a 2012 contract included in court documents that indicates Lieber received $50,000 a month in salary and millions of dollars in research support. "That is a corrupting level of money."

Federal investigators were also alarmed, Lelling says, by how Lieber "brazenly" hid that relationship from Harvard and from the federal agencies that for decades have been funding his research on inorganic nanowires. "When people begin to hide things, that's when law enforcement authorities get all excited."

SIGN UP FOR OUR DAILY NEWSLETTER
Get more great content like this delivered right to you!

Email Address *

"A little bit of fear"

Lieber is the highest profile scientist arrested so far. On 28 January, DOJ announced he is one of three people from Boston facing charges related to China. The other two—a junior cancer researcher at Beth Israel Deaconess Medical Center and a former undergraduate student at Boston University (BU)—are both Chinese nationals.

Born and trained in the United States, Lieber is a member of both the U.S. national academies of sciences and medicine. At Harvard since 1991, he has pioneered work on the chemical synthesis of nanowires and their incorporation into devices ranging from transistors to light emitters and sensors. Most recently, his lab developed soft, flexible nanowire nets that could be injected into the brains or retina of animals to unfurl and wrap around neurons, and then eavesdrop on the electrical communication between cells. In 2011, he began a collaboration with Wuhan University of Technology (WUT) in China that is at the center of his alleged violations. (WUT did not respond to requests for comment on its relationship with Lieber.)

Lieber was released on 30 January after posting a $1 million bond and agreeing to remain in Massachusetts. He has been suspended with pay from Harvard, which last week called the charges "extremely serious" and said it is "cooperating with federal authorities." His lawyer, Peter Levitt, declined to comment on the charges.

Lelling says Lieber's prominence was not a "deciding factor" in DOJ's decision to file criminal charges. "This wasn't about looking for a bigger scalp," Lelling insists. But, "The fact that Lieber is a prominent academic helps us to get out our message … that transparency works," he adds.

Lelling says the DOJ team works closely with the National Institutes of Health (NIH), which has been much more aggressive than other federal research agencies in pursuing apparent violations of federal policy requiring disclosure of foreign research support. Over the past 18 months, NIH has asked more than 60 grantee institutions to investigate what it has flagged as questionable behavior by some 200 faculty members, notably participation in China's Thousand Talents Program. Lieber signed up for Thousand Talents in 2012, according to court documents. Although both NIH and the universities have generally stayed quiet about their responses to those letters, at least 15 scientists have resigned or been dismissed at a half-dozen institutions that have spoken publicly about their actions.

"I think those letters have had an *in terrorem* effect," Lelling says, using a legal term for how the threat of prosecution can scare people into following the law. "And that's good, because you want a little bit of fear out there to sensitize people to the magnitude of the problem."

Charles Lieber REUTERS/KATHERINE TAYLOR

"All across the spectrum"

DOJ weighs several factors in deciding which cases to bring forward, according to Lelling. "Is there deception?" he asks. "How much money was involved? What kind of technology was transferred?" And what other steps did a researcher take to develop the relationship?"

Lelling says he understands the research community's confusion over exactly what types of behavior could result in criminal charges and what scientists should do to avoid that fate. "I agree that the responses of universities to this kind of behavior have been all across the spectrum," Lelling told *Science*Insider. "And obviously, we don't control what the universities do."

The challenge for DOJ, he says, is to attack the problem vigorously without being heavy-handed. "There may be situations in which a professor has done something that doesn't quite reach the level of charging them with a federal felony," Lelling says. "So maybe the federal authorities say to the university, 'You should deal with that.' And the university says, 'OK, OK, we'll do it.'"

The China Initiative's working group meets regularly to "come up with consistent messaging," Lelling says. And that includes prodding the department's 89 field offices "to be aggressive, because we want them to prioritize these cases." At the same time, Lelling says, he and his colleagues are aware that

Shifting loyalties

Lelling rejects criticism that the department has unfairly targeted ethnic Chinese people and other Asian Americans. "Dr. Lieber is probably the most prominent academic charged in this kind of case so far," Lelling says, "and he is not a Chinese national, nor is he of Chinese descent." But Lelling says China's aggressive efforts to become the world leader in many high-tech fields has meant devoting more resources to tracking those of Chinese ancestry.

"The bottom line is that this is an effort by a rival nation state to steal U.S. technology," Lelling says. "And that rival nation is made up almost exclusively of Han Chinese. And so, unfortunately, a lot of our targets are going to be Han Chinese. If it were the French government targeting U.S. technology, we'd be looking for Frenchmen."

Lelling recognizes that international collaboration has helped make U.S. science the envy of the world, and thinks that U.S.-trained scientists should be free to live and work anywhere. But those who decide to mingle their federal funding with support from Chinese institutions are playing a dangerous game, he warns, adding that Lieber is a perfect example.

"The Chinese government has a very strategic approach to obtaining technology," Lelling says. "It targets researchers who specialize in areas where the Chinese are deficient, in the hopes that they can piggyback on their expertise to close that strategic gap."

"What concerns us ... is that a scientist who accepts their support becomes dependent on it to the point where they are willing to accept [an assignment] from the Chinese government or a Chinese university for whatever it is they need. Those of us that work on public corruption cases develop a radar for when person or entity A is attempting to coopt or corrupt person or entity B. And a large enough amount of money can shift loyalties."

Getting over the hump

Lelling says the two other people charged last week are outliers in the China Initiative's portfolio.

Ye Yanqing, a 29-year-old former BU student who the U.S. government alleges is a lieutenant in the Chinese military, is charged with lying about her military affiliation on her visa documents. Such cases involving foreign intelligence officers are rare, Lelling says. Zheng Zaosong, a 30-year-old cancer researcher, has been charged with trying to smuggle 21 vials of biological material out of the country and lying about the contents of his suitcase when confronted by federal airport security agents. Ye is believed to be back in China, while Zheng has been detained since 30 December 2019.

Looking ahead, Lelling expects to prosecute more cases of scientists who have failed to disclose their Chinese ties. But he thinks the number of cases will then drop as universities absorb what they have learned from interactions with officials from various federal law enforcement, intelligence, and national security agencies.

"The universities have been extremely responsive," he says. "They are becoming sensitized to the problem. So, after we get over a little hump here, I think things will rapidly improve."

With reporting by Dennis Normile and Robert F. Service.

Posted in: **Asia/Pacific**, **Scientific Community**
doi:10.1126/science.abb1489

Jeffrey Mervis
Jeff tries to explain how government works to readers of *Science*.
Email Jeffrey

More from News

'I can't even enjoy this.' #BlackBirdersWeek organizer shares her struggles as a black scientist

Prominent Harvard archaeologist put on leave amid allegations of sexual harassment

'I would not recommend this.' A scientist's hydroxychloroquine trial—and his advice to Trump

Science's extensive COVID-19 coverage is free to all readers. To support our nonprofit science journalism, please **make a tax-deductible gift today.**

Earth's species disappearing at an alarming rate
By Amanda Heidt | Jun. 4, 2020

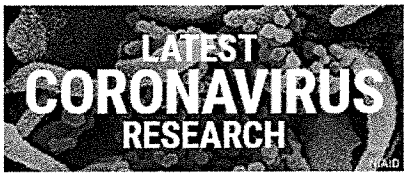
Watch an example of chimpanzee 'culture,' as one fishes for termites
By Amanda Heidt | May. 28, 2020

Our Moon is not as 'dry' as we thought
By Amanda Heidt | May. 8, 2020

Herpes virus can trigger Alzheimer's, brain tissue study suggests
By Kelly Servick | May. 7, 2020

Cancer drug dampens intrusive thoughts in men with pedophilic disorder
By Amanda Heidt | May. 1, 2020

More Sifter



Read the Latest Issue of *Science*

5 June 2020

Vol 368, Issue 6495

Table of Contents

ASTRONOMY
Double trouble

SCIENTIFIC COMMUNITY
Bill would supersize NSF's budget—and role

EUROPEAN NEWS
Europe bets R&D spending will bring jobs to battered economy

SCIENTIFIC COMMUNITY
Shuttered natural history museums fight for survival

MEDICINE/DISEASES
The pandemic's first major research scandal erupts

MEDICINE/DISEASES
Blood vessel injury may spur disease's fatal second phase

Get Our E-Alerts

Receive emails from *Science*. See full list

- ☑ *Science* Table of Contents
- ☑ *Science* Daily News
- ☑ Weekly News Roundup
- ☑ *Science* Editor's Choice
- ☑ First Release Notification
- ☑ *Science* Careers Job Seeker

United States

Email address*

Advertisement

Latest News

Trending

1. A mysterious company's coronavirus papers in top medical journals may be unraveling
2. Blood vessel attack could trigger coronavirus' fatal 'second phase'
3. Why coronavirus hits men harder: sex hormones offer clues
4. Urban foxes may be self-domesticating in our midst
5. Eye, robot: Artificial intelligence dramatically improves accuracy of classic eye exam

Most Read

1. A mysterious company's coronavirus papers in top medical journals may be unraveling
2. Study that claims white police no more likely to shoot minorities draws fire
3. Why do some COVID-19 patients infect many others, whereas most don't spread the virus at all?

Required fields are indicated by an asterisk (*)

© 2020 American Association for the Advancement of Science. All rights Reserved. AAAS is a partner of HINARI, AGORA, OARE, CHORUS, CLOCKSS, CrossRef and COUNTER.

Terms of Service
Privacy Policy
Contact AAAS

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 Trends In Criminal Trade Secret Prosecution

By **Jessica Nall and Janice Reicher** (January 23, 2019, 1:39 PM EST)

Jessica Nall

Janice Reicher

Criminal trade secret prosecutions are on the rise nationwide and in the Northern District of California, especially cases relating to alleged theft by Chinese nationals and entities. According to a 2017 report by the White House Office of Trade and Manufacturing Policy, Chinese theft of American intellectual property costs between $225 billion and $600 billion annually.[1]

On Nov. 1, 2018, former Attorney General Jeff Sessions announced the U.S. Department of Justice's new "China Initiative," designed to "identify priority Chinese trade theft cases, ensure that we have enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively."[2] Since that announcement, the DOJ has prosecuted numerous cases related to alleged Chinese theft of trade secrets under the Economic Espionage Act (18 U.S.C. 1831, et. seq.), accelerating a trend already in place.

Criminal prosecutions for trade secret theft involving no foreign component at all are also on an uptrend. These cases involve private actors that are U.S.-based with no national security implications. Finally, criminal trade secret prosecutions following parallel civil actions are becoming more commonplace. These major trends are discussed below.

A Spike in Prosecutions of Criminal Trade Secret Cases Related to China

While announcing the China Initiative on Nov. 1, the DOJ also revealed that it was bringing a case involving the alleged theft of Micron trade secrets: "a grand jury in San Francisco has returned an indictment alleging economic espionage on the part of a Chinese state-owned, government owned, company, a Taiwan company, and three Taiwan individuals for an alleged scheme to steal trade secrets from Micron, an Idaho-based semi-conductor company."

The case is United States v. United Microelectronics Corp.[3] The corporate defendants were arraigned on Jan. 9, 2019, and both pleaded not guilty. This case is being watched closely because it is the first one brought under the China Initiative, and the government is reportedly employing novel tactics in prosecuting it.[4] For the first time, the government has filed a simultaneous civil lawsuit under the Economic Espionage Act in addition to the criminal indictment.[5] In the civil case, the government aims to block the Chinese corporate defendant from exporting dynamic random access memory, alleging that it contains Micron's trade secrets.[6] Meanwhile, prosecution-friendly revisions to Federal Rule of Criminal Procedure 4 have allowed for easier service on foreign corporate defendants.[7]

The statistics on economic espionage cases involving China in the past several years are staggering. While announcing the indictment of two computer hackers associated with the Chinese government on Dec. 20, 2018, Deputy Attorney General Rod Rosenstein noted that "[m]ore than 90 percent of the Department's cases alleging economic espionage over the past seven years involve China. More than two-thirds of the Department's cases involving thefts of trade secrets are connected to China."[8]

The very next day, on Dec. 21, the DOJ announced that a Chinese national had been arrested in the Northern District of Oklahoma for stealing trade secrets from his employer, a U.S.-based petroleum company. The alleged trade secrets relate to a product valued at over $1 billion regarding the manufacture of a "research and development downstream energy market product."[9] Assistant Attorney General for National Security John C. Demers stated: "The theft of intellectual property harms American companies and American workers. As our recent cases show, all too often these thefts involve the Chinese government or Chinese companies. The Department recently launched an initiative to protect our economy from such illegal practices emanating from China, and we continue to make this a top priority."[10]

Unsurprisingly given its proximity to the Pacific Rim and as home to a plethora of major technology companies, the Northern District of California in particular has become a hotbed for criminal trade secret prosecutions. In July 2018, the U.S. Attorney's Office for the Northern District indicted a former Apple Inc. employee for theft of trade secrets in violation of 18 U.S.C. § 1832.[11] The employee was arrested at San Jose Airport as he attempted to board a flight to China.

The government alleges that he downloaded numerous documents from Apple's server prior to resigning, including a confidential 25-page document containing detailed schematic drawings of a circuit board designed to be used in the critical infrastructure of a portion of an autonomous vehicle. They allege that he left Apple under false pretenses to join an autonomous vehicle technology company headquartered in China.

Then in September 2018, four Chinese state-owned industrial companies were arraigned on an indictment charging them and two of their officers with economic espionage in conspiring to acquire stolen or misappropriated technology trade secrets from DuPont Co.[12]

In October 2018, the government also issued indictments against four former Genentech Inc. employees accused of stealing confidential Genentech trade secrets in order to assist a company in Taiwan in creating and selling drugs similar to Genentech's.[13]

If this trend continues we can expect to see several more China-related criminal trade secret cases in the Northern District by the end of 2019.

A Growing Willingness to Prosecute Cases With No Foreign Actor or National Security Interest

While trade secret prosecutions connected to China are a major focus, a related trend has also simultaneously emerged: the DOJ's increased willingness to bring trade secret cases involving no foreign actor or national security concern. The DOJ's Justice Manual lists several discretionary factors to be considered in deciding whether to initiate a prosecution under the Economic Espionage Act, including: "(a) the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality; (b) the degree of economic injury to the trade secret owner; (c) the type of trade secret misappropriated; (d) the effectiveness of available civil remedies; and (e) the potential deterrent value of the prosecution."[14]

In recent years, the significance of factor (a) regarding the involvement of a foreign actor in the alleged crime appears to be shifting. Benjamin B. Wagner, the former United States attorney for the Eastern District of California, discussed this trend at a September 2018 trade secrets conference in San Francisco. He explained that the U.S. attorney's office historically has been reluctant to take cases when one private actor has a civil action pending or threatened against another private actor, and where there is no foreign actor or national security interest to protect.[15] The DOJ was traditionally loath to be seen as having been dragged into civil litigation and used as a weapon by one company against another.

According to Wagner, this reticence has receded gradually over the years, and the DOJ is now more willing to take such cases as the value of the U.S. economy is much more tied to intellectual property than it was 20 ago. In other words, the protection of intellectual property rights has significant economic consequences, and the involvement of prosecutors in otherwise private, civil disputes could be perceived as increasingly warranted depending on the case. In Wagner's estimation, there is still probably only a 50 percent chance that a U.S. attorney would file a case with only private civil actors involved, though this is a substantial increase from the previous likelihood of just 20 percent.

A recent example of the trend toward domestic-focused trade secret prosecutions in the Northern District of California is United States v. Mogal.[16] In June 2018, the U.S. attorney's office indicted six former employees of a defunct fitness tracker company, Jawbone, alleging that they possessed Jawbone trade secrets after their employment with Jawbone ended and they accepted employment with Fitbit Inc.[17] The indictment contains no allegation of "evidence of involvement by a foreign government, foreign agent or foreign instrumentality."[18]

In addition, the high-profile civil trade secret theft case between Uber Technologies Inc. and Waymo LLC has apparently led to a criminal investigation of Uber, though no indictment has yet been issued.[19] In February 2017, Google subsidiary Waymo alleged that Anthony Levandowski, a former employee, stole trade secrets regarding driverless cars from Google before leaving and using that information for Uber's benefit. The companies settled the civil case in February 2018, but the DOJ confirmed that it had opened a criminal investigation of Uber after the federal judge in the civil action referred the case to the U.S. attorney's office.[20]

An Increase in Criminal Trade Secret Prosecutions Following Parallel Civil Cases

Following the announcement of a criminal investigation or indictment, it is common for private plaintiffs to capitalize on the government's work and file civil suits against the same defendants. However, the dispute between Waymo and Uber highlights another trend: the rise of criminal trade secret prosecutions that follow parallel civil cases.

The DOJ's criminal investigation of Uber may have arisen out of unusual circumstances, namely the direct referral of the case from the federal judge in the civil case to the U.S. attorney's office. However, the practice of prosecutors filing criminal trade cases alongside parallel civil actions, or following civil actions, has become more common in recent days.

For example, prosecutors filed the Mogal criminal case against former Jawbone employees after Jawbone had already litigated civil actions against Fitbit for trade secret misappropriation, including in the U.S. International Trade Court and San Francisco Superior Court.[21] Similarly, with regard to United States v. United Microelectronics Corp., prosecutors issued the indictments after a parallel civil case[22] by Micron against UMC had been under way for almost a year. In both cases, there was already an extensive civil-case record upon which prosecutors could rely for the subsequent criminal cases if they chose to do so.

In some cases, "victim" companies will even make presentations to prosecutors to convince them to take a case in order to increase their leverage in the civil litigation. The rise of these follow-on prosecutions may suggest that prosecutors are weighing the factor of "the effectiveness of available civil remedies" less heavily in making their charging decisions.[23]

Conclusion

While white collar filings are significantly down nationwide, one area of white collar prosecutions appears to be expanding quickly, especially in the Northern District of California. The prosecutorial appetite for bringing criminal trade secret cases, especially relating to China, appears voracious. Even where no foreign actor or national security concern is involved, or where a dispute among two private actors has been (or is being) fully litigated in a civil forum, the DOJ may still be more inclined than ever to bring a criminal investigation or action. At the same time, legislative revisions such as the changes to Federal Rule of Criminal Procedure 4 to allow for easier service on foreign corporate defendants and related precedent that has developed around it[24] are facilitating trade secret prosecutions against foreign actors. All signs indicate that there is much more to come.

Jessica K. Nall is a partner and Janice W. Reicher is a senior associate at Farella Braun & Martel LLP.

Disclosure: In United States v. United Microelectronics Corp., Farella Braun serves as counsel for one of the individual defendants from UMC who has not yet appeared in the action. In United States v. Mogal, the firm serves as counsel for defendant Rong Zhang. Only public information regarding the case is provided in this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] White House Office of Trade and Manufacturing Policy, How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World, Whitehouse.gov at p.5 (June 2018), https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf (citing The Comm'n on the Theft of Amer. Intellectual Prop., The Nat'l Bureau of Asian Research, ipcommission.org at 1 (2017), http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf).

[2] U.S. Department of Justice, Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage, justice.gov (November 1, 2018), https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

[3] United States v. United Microelectronics Corp. (UMC), Case No. 3:18-cr-00465 MMC (N.D. Cal.). The authors' law firm serves as counsel for a defendant in this case. Only public information regarding the case is provided in this article.

[4] Joel Rosenblat, U.S. Deploys New Tactics in Prosecution of Chinese Chipmaker, Bloomberg (Jan. 9, 2019 4:00 PM), https://www.bloomberg.com/news/articles/2019-01-09/u-s-deploys-new-tactics-in-prosecution-of-chinese-chipmaker.

[5] Id.

[6] Id.

[7] In addition, federal prosecutors received a boost when the Ninth Circuit affirmed in the 2017 case against Chinese-government-owned Pangang Group that the company had been properly served a criminal summons through its U.S. counsel, after its U.S. counsel appeared on its behalf in court solely to contest the service and admitted the company's actual knowledge of the summons. The basis for the ruling was Federal Rule of Criminal Procedure 4, which was revised in 2016 to allow "an organization not within a judicial district of the United States," to be served by, among other methods, "any other means that gives notice . . . ." Fed. R. Crim. P. 4(c)(3)(D). Tiffany Hu, 9th Circuit Says Chinese Co. Given Notice In Trade Secrets Row, Law360 (Aug. 23, 2018 4:09 PM), https://www.law360.com/articles/1076084/9th-circ-says-chinese-co-given-notice-in-trade-secrets-row.

[8] U.S. Department of Justice, Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers, justice.gov (Dec. 20, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers.

[9] U.S. Department of Justice, Chinese National Charged with Committing Theft of Trade Secrets, justice.gov (Dec. 21, 2018), https://www.justice.gov/opa/pr/chinese-national-charged-committing-theft-trade-secrets.

[10] Id.

[11] U.S. Department of Justice, Former Apple Employee Indicted on Theft of Trade Secrets, justice.gov (July 16, 2018), https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets.

[12] U.S. Department of Justice, Four Chinese State Owned Industrial Companies Arraigned in Economic Espionage Conspiracy, justice.gov (Sept. 7, 2018), https://www.justice.gov/usao-ndca/pr/four-chinese-state-owned-industrial-companies-arraigned-economic-espionage-conspiracy.

[13] U.S. Department of Justice, Former Genentech Employees Charged With Theft of Trade Secrets, justice.gov (Oct. 29, 2018), https://www.justice.gov/usao-ndca/pr/former-genentech-employees-charged-theft-trade-secrets.

[14] Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1837)—Prosecutive Policy, Justice Manual, § 9-59.100, https://www.justice.gov/jm/jm-9-59000-economic-espionage.

[15] 2018 Update, Two Years After DTSA, 800 Cases Trade Secrets Protection, Enforcement and Litigation Panel (Sept. 27, 2018).

[16] United States v. Mogal, et al., Case No. 5:18-cr-00259-BLF (N.D. Cal).

[17] U.S. Department of Justice, Six Former and Current Fitbit Employees Indicted for Possessing Multiple Trade Secrets Stolen from Jawbone, justice.gov (June 14, 2018), https://www.justice.gov/usao-ndca/pr/six-former-and-current-fitbit-employees-indicted-possessing-multiple-trade-secrets.

[18] See supra, n.13.

[19] Mike Isaac, Uber Under Criminal Investigation, Justice Dept. Confirms in Letter to Court, nytimes.com (Dec. 13, 2017), https://www.nytimes.com/2017/12/13/technology/uber-waymo-driverless-cars.html.

[20] Id.

[21] Melissa Daniels, Fitbit Cleared of Jawbone's Trade Secret Claims at ITC, Law360 (Oct. 20, 2016 10:21 PM), https://www.law360.com/articles/854094/fitbit-cleared-of-jawbone-s-trade-secret-claims-at-itc.

[22] Micron v. United Microelectronics Corp. , Case No. 3:2017cv06932 (N.D. Cal.).

[23] See supra, n.14

[24] See supra, n.7.

All Content © 2003-2020, Portfolio Media, Inc.

Accused of Spying for China, Until She Wasn't

By Nicole Perlroth

May 9, 2015

On Monday, Oct. 20, 2014, Sherry Chen drove, as usual, to her office at the National Weather Service in Wilmington, Ohio, where she forecast flood threats along the Ohio River. She was a bit jet-lagged, having returned a few days earlier from a visit to China. But as she headed to her desk, she says, she had no reason to think it was anything other than an ordinary day. Then her boss summoned her.

Once inside his office, a back door opened and in walked six agents from the Federal Bureau of Investigation.

The agents accused Mrs. Chen, a hydrologist born in China and now a naturalized American citizen, of using a stolen password to download information about the nation's dams and of lying about meeting with a high-ranking Chinese official.

Mrs. Chen, 59, an adoptive Midwesterner who had received awards for her government service, was now suspected of being a Chinese spy. She was arrested and led in handcuffs past her co-workers to a federal courthouse 40 miles away in Dayton, where she was told she faced 25 years in prison and $1 million in fines.

Her life went into a tailspin. She was suspended without pay from her job, and her family in China had to scramble for money to pay for her legal defense. Friends and co-workers said they were afraid to visit. Television news trucks parked outside her house, waiting to spot a foreign spy hiding in plain sight in suburban Wilmington, population 12,500.

"I could not sleep," Mrs. Chen said in a recent interview. "I could not eat. I did nothing but cry for days."

Then, five months later, the ordeal abruptly ended. In March, just a week before she was scheduled to go on trial, prosecutors dropped all charges against Mrs. Chen without explanation.

"We are exercising our prosecutorial discretion," said Jennifer Thornton, the spokeswoman for the United States attorney for the Southern District of Ohio. She added that last year the Justice Department filed 400 indictments and "criminal informations" — charges filed in connection with plea agreements — and dismissed 13 of them, including Mrs. Chen's. The United States attorney would not comment on the investigation, but there is little question that law enforcement is facing new pressure to pursue any lead that could be related to trade-secret theft.

For the last few years, government officials have noted with growing alarm that Chinese hackers and paid insiders were spiriting trade secrets and other confidential information out of the United States. The mantra, these days, is that there are only two types of companies left in this country: those that have been hacked by China, and those that do not know they have been hacked by China.

In 2013, President Obama announced a new strategy to fight back. The cornerstone was more aggressive investigations and prosecutions, and Justice Department prosecutions under the Economic Espionage Act jumped more than 30 percent from the year before. During the first nine months of 2014, the total increased an additional 33 percent. Notably, more than half of the economic espionage indictments since 2013 have had a China connection, public documents show.

It was in this climate that prosecutors zeroed in on Mrs. Chen.

"They came across a person of Chinese descent and a little bit of evidence that they may have been trying to benefit the Chinese government, but it's clear there was a little bit of Red Scare and racism involved," said Peter J. Toren, a former federal prosecutor who specialized in computer crimes and industrial espionage. He is now a partner at Weisbrod Matteis & Copley in Washington, and the author of "Intellectual Property and Computer Crimes."

Interviews with Mrs. Chen and her former colleagues and a review of court filings, which include a year's worth of Mrs. Chen's work and personal emails, suggest that prosecutors hunted for evidence of espionage, failed and settled on lesser charges that they eventually dropped.

"The government thought they had struck gold with this case," said Mark D. Rasch, a former Justice Department espionage and computer-crimes prosecutor who reviewed the case. "The problem was the facts didn't quite meet the law here."

A Favor Gone Wrong

Mrs. Chen, whose given name is Xiafen, was born in Beijing. From an early age, she was an engineering type. An uncle encouraged her to pursue a career in building design, but she says she was more interested in the abstract nature of water and air. "You can't see them with your own two eyes," she said, growing animated. "It's so much more complex than that. I found it fascinating."

Peter R. Zeidenberg, Ms. Chen's lawyer.

Greg Kahn for The New York Times

She earned advanced degrees in hydrology in Beijing, married and moved to the United States to pursue a degree in water resources and climatology at the University of Nebraska. She became an American citizen in 1997. After 11 years working for the state of Missouri, she took the job at the weather service in Ohio in 2007.

In Wilmington, she and her husband, an electronics specialist, moved into a ranch-style house a short drive from her office, settling into a life of comfortable routine.

Ask Mrs. Chen about her home or hobbies and you may get a word or two. Ask her about water flow or the Ohio River and she will talk for hours. Some 25 million people live along the Ohio River basin, which runs more than 900 miles from Pittsburgh to Cairo, Ill., where it joins the Mississippi River. Along the way, it flows through locks and dams operated by the United States Army Corps of Engineers. Mrs. Chen developed a forecasting model for predicting floods along the Ohio and its tributaries. The model involves constant data-gathering about water levels and rainfall, as well as how dam and lock operators respond to water flow.

Mrs. Chen was known to be tenacious in her pursuit of data for her predictions. She developed carpal-tunnel syndrome in her right hand from eight years of repetitive mouse clicks. Thomas Adams, who hired Mrs. Chen at the National Weather Service in 2007, said her fascination with data made her perfect for the job.

"Sherry is and was dedicated to getting the details right — and that matters significantly," Mr. Adams said, noting that one inch of water could make the difference between a levee holding or failing.

Mrs. Chen would return to Beijing every year to visit her parents, which is how her troubles began. During her 2012 trip, a nephew said that his future father-in-law was in a payment dispute with provincial officials over a water pipeline.

The nephew knew that one of Mrs. Chen's former hydrology classmates, Jiao Yong, had become vice minister of China's Ministry of Water Resources, which oversees much of China's water infrastructure. As Mrs. Chen tells it, her nephew asked her to reach out to Mr. Jiao, hoping he might be able to help his future wife's father. Mrs. Chen said she was reluctant to do so since she had not seen Mr. Jiao in many years, but ultimately contacted him.

Mr. Jiao's secretary set up a 15-minute chat in his office in downtown Beijing, and Mr. Jiao said he would try to intercede. As their conversation wound down, he also mentioned that he was in the process of funding repairs for China's aging reservoir systems and was curious how such projects were funded in the United States.

It was a casual question, Mrs. Chen said, but she was embarrassed not to know the answer. As a young hydrology student in China, she had been well versed in water project finance. It was not until that moment, she said, that she realized how little she knew about financing of such projects in her new home country.

Always a master of details, she said her ignorance in this case gnawed at her.

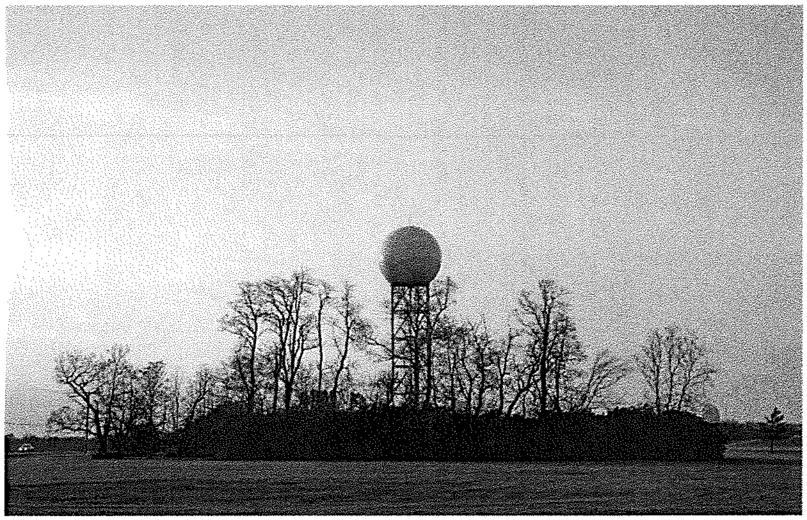
When she returned to Ohio, she set out to find an answer. She eventually sent Mr. Jiao an email with links to websites, but nothing directly relevant to his question.

She also asked for help from Deborah H. Lee, then the chief of the water management division at the Army Corps of Engineers, with whom Mrs. Chen had worked on projects over the years.

Copies of emails included in court documents show that Ms. Lee directed Mrs. Chen to her agency's website and told her that if her former classmate had further questions, he could contact her directly. Mrs. Chen then sent a second, final email to Mr. Jiao instructing him to call Ms. Lee directly with any additional questions.

Shortly after her email exchange with Mrs. Chen, Ms. Lee reported their correspondence to security staff at the Department of Commerce, the agency over the National Weather Service. "I'm concerned that an effort is being made to collect a comprehensive collection of U.S. Army Corps of Engineers water control manuals on behalf of a foreign interest," Ms. Lee wrote.

Ms. Lee would not comment on her motivations for sending the email. Last September, she left the Army Corps of Engineers for a job at the National Oceanic Atmospheric Administration. A spokeswoman for N.O.A.A. said neither Ms. Lee nor the agency would comment on what they deemed a "personnel matter."



A radar tower in Wilmington, Ohio, used by the National Weather Service, where Ms. Chen worked. Ty Wright for The New York Times

If Mr. Jiao was trying to recruit Mrs. Chen, he was awfully lackadaisical about it. It took a week to respond to her first email. "Hi Xiafen: Your email received," he wrote, in English. "Thanks for information you forward me. I will go through it." His second email was briefer: "Thanks a lot."

That was the extent of their correspondence, according to findings of a search warrant for Mrs. Chen's work and personal email records.

Mrs. Chen said she never did find out whether Mr. Jiao had helped her nephew's father-in-law, and has not heard from him since. Mr. Jiao did not respond to requests for comment.

But in her search for an answer to Mr. Jiao's question, Mrs. Chen had gone through the National Inventory of Dams database. That database, which is maintained by the Army Corps of Engineers, is available to government workers and members of the public who request login credentials. A small subset of the data on the site — six of 70 data fields — is available only to government workers.

As a government employee, Mrs. Chen would have had full access to the database. But she didn't have a password; the government began requiring passwords in 2009, after the last time Mrs. Chen had used it. So she asked a colleague, Ray Davis, in the adjacent cubicle, for help. Mr. Davis, who had already provided the password and login instructions to the whole office, emailed the password to her.

Mrs. Chen didn't find much useful information for Mr. Jiao, but did download data about Ohio dams that she thought could be relevant to her forecasting model. For Mr. Jiao, she included a link to the database in her second email and noted that "this database is only for government users, and nongovernment users are not able to download any data from this site." If he had any questions, or needed information, she told him, he should contact Ms. Lee — who had just reported Mrs. Chen as a possible spy.

When Mr. Davis was later questioned by Commerce officials, he said he did not remember giving Mrs. Chen a password. Mrs. Chen said she did not remember receiving one. And neither believed they had done anything wrong, according to reports of their interviews.

The password, however, would come to haunt her. Nearly a year after Ms. Lee's tip, Mrs. Chen was visited at her office by two special agents from the Commerce Department. They interrogated her for seven hours about the password, and her 15-minute meeting with the Chinese official.

Asked when she last met with Mr. Jiao, she responded, "It was the last time I visited my parents, I think 2011, May 2011."

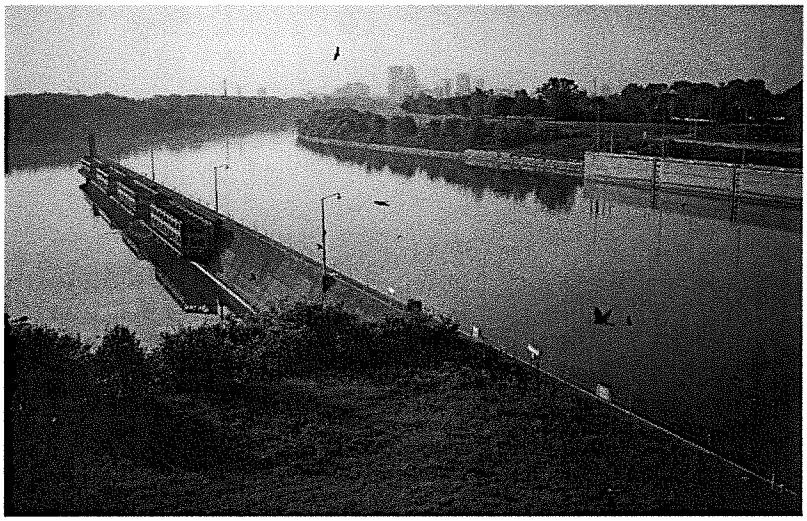
That was June 2013. Mrs. Chen did not hear from the government for another three months, when she and her husband returned from a four-week trip to see her parents. Her father, who had been ill, died during the visit. The day after she returned, the Commerce Department agents showed up at her office.

A slow-motion investigation was gathering momentum. An F.B.I. memo regarding Mrs. Chen, dated July 11, 2014, listed the Army Corps of Engineers as "victim — economic espionage — PRC," short for People's Republic of China.

In September 2014, Mrs. Chen and her husband were stopped while boarding a United Airlines flight to Beijing from Newark. Their baggage was pulled and searched. Ms. Chen said they were ultimately allowed to return to the plane, which had been held for over an hour.

It was after returning from that trip, in October, that she was arrested. At the Dayton courthouse, she was charged with four felonies, including that she had illegally downloaded data about "critical national infrastructure" from a restricted government database — the National Inventory of Dams — and made false statements.

The false statement referred to telling the agents that she had last seen Mr. Jiao in 2011, not 2012. Four other charges were added later.



The upriver entrance to the McAlpine Locks along the Ohio River. Ms. Chen was accused of using a stolen password to download information about the nation's dams and of lying about meeting with a high-ranking Chinese official. Luke Sharrett for The New York Times

She was released the same day and placed on unpaid administrative leave.

'Why Would You Do That?'

After the arrest, Mrs. Chen's name was all over the Internet. The case was picked up by local media and The Washington Free Beacon, a conservative news website, which played up Mrs. Chen's meeting with a "senior Chinese official."

Mrs. Chen says she was living a nightmare. Peter R. Zeidenberg, a partner at Arent Fox in Washington who represented Mrs. Chen, said he believed it was telling that the government went after Mrs. Chen for using a colleague's password, but not after the colleague who gave it to her — and to the entire office. (Neither Mr. Davis nor anyone else currently employed at the National Weather Service would comment for this article.)

Mr. Adams, her former colleague, said he thought that Mrs. Chen's Chinese background played a role. "If this had been you or me or someone of European descent who borrowed someone else's password," he said, "they would have said, 'Don't do this again.' " He added: "This is the gratitude the government has shown for her hard work and dedication as a federal public servant. It's shameful."

A week before trial was to begin, Mr. Zeidenberg requested a meeting with Carter M. Stewart and Mark T. D'Alessandro, two United States attorneys for the Southern District of Ohio.

"Why," Mr. Zeidenberg said he asked, "if she's a spy, is she coming back from China and telling her colleagues that 'I met this guy in China and this is what he wants to know'? Why is she telling the guy in China, 'Here's my boss's phone number'? Why is she asking for a password over email? Why would you do that?"

Mr. Zeidenberg says the prosecutors listened. On March 10, the day after their meeting, they dismissed the charges.

"Thank God," Mr. Zeidenberg added.

Looking Everywhere for Spies

Mrs. Chen was caught in a much broader dragnet aimed at combating Chinese industrial espionage. Law enforcement investigations into trade-secret theft are now at record levels, jumping 60 percent between 2009 and 2013, according to an F.B.I. report last year.

Accused of Spying for China, Until She Wasn't - The New York Times

In 2013, Eric H. Holder Jr., then the attorney general, said the Justice Department would bring more economic espionage cases, and in 2014 it secured the first ever indictment of foreign actors when it charged five Chinese military officers with trade-secret theft. (The chances of arrests, however, are slim.)

Inside the United States, prosecutors recently invoked the Foreign Intelligence Surveillance Act in the case of a Chinese citizen living in this country accused of stealing hybrid seeds from an Iowa cornfield. In addition to physical surveillance, the government used a secret FISA warrant to intercept the defendant's mail, email and phone calls and install location-tracking and listening devices in his car.

In another case, in Philadelphia, an American resident with Chinese citizenship stands accused of damaging a server to cover up trade-secret theft. He's been held in a federal detention center for over two years; his trial is set for November.

"If you're looking everywhere for spies, you will find spies everywhere, even where they don't exist," said Mr. Rasch, the former computer-crimes prosecutor.

The case against Mrs. Chen has made her wary. After I had interviewed her several times but did not contact her for some days, she said she had convinced herself that I was not a reporter at all, but an undercover agent.

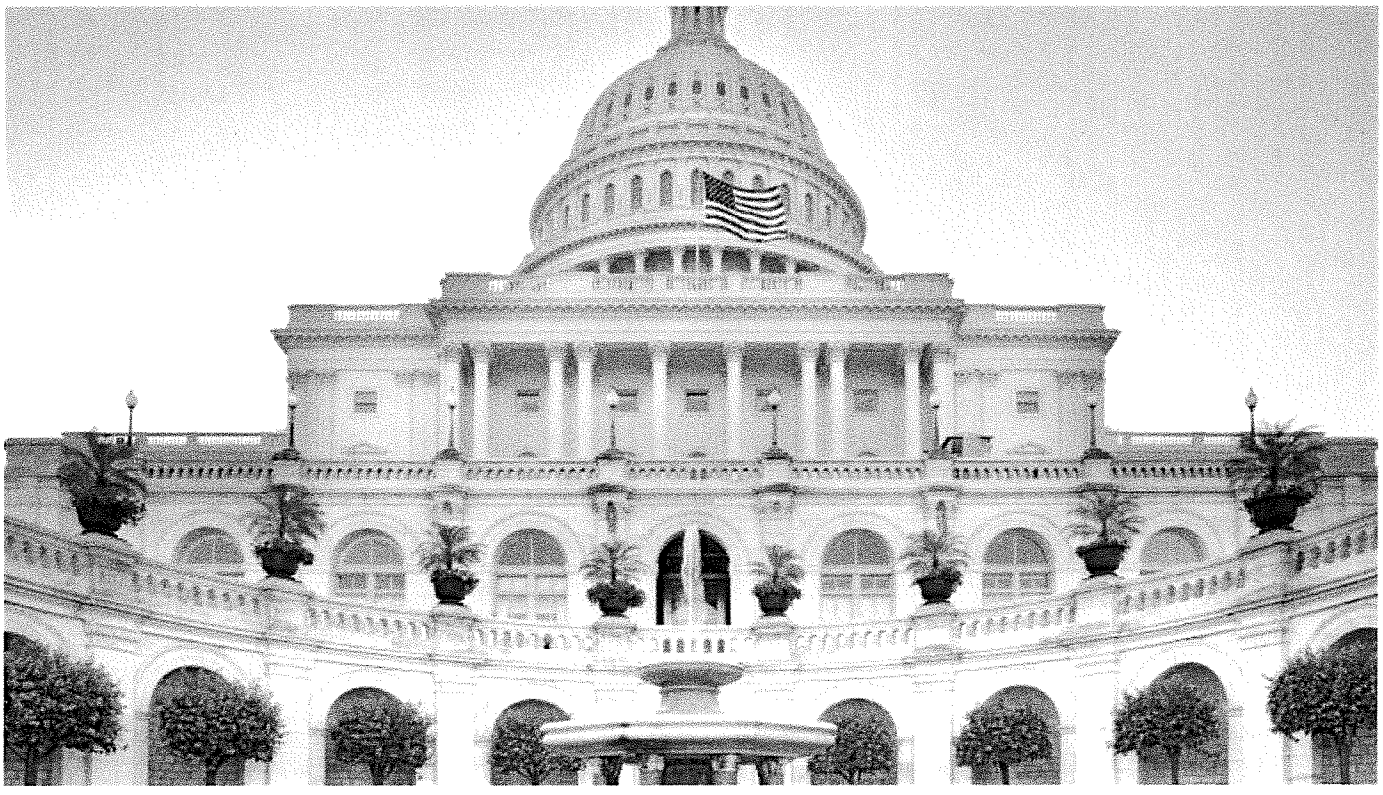
Mrs. Chen says she recalls becoming an American citizen as her proudest moment. She told me about all the positive performance reviews she received and began to cry when she remembered the way she was handcuffed in front of co-workers and put into the back of an F.B.I. car.

Still, she says, she wants her job back. "I know they treated me unfairly, but I'm proud of my service," she said. "The forecasting model is very important. I miss my colleagues. I miss my work. It's my life."

Mrs. Chen's benefits and pay have been restored, but she is waiting to hear whether the Commerce Department will allow her to return to work. Sara Ryan, the department lawyer handling Mrs. Chen's case, said she would not discuss it. Representatives for the department did not return requests for comment.

Asked whether he thought Mrs. Chen should get her job back, Mr. Adams, her former colleague, said he was torn. "I want her to get her job back as soon as possible," he said. "But on the other hand, I also hope she never goes back there again. After the way she was treated, she should be concerned that the government hasn't given up the ghost."

REP LIEU CALLS ON FBI DIRECTOR TO CLARIFY STATEMENTS ON CHINESE ACADEMICS



February 15, 2018 Press Release

WASHINGTON- Today, Congressman Ted W. Lieu (D-Los Angeles County) issued the following statement after it was reported (https://www.thedailybeast.com/fbi-directors-shock-claim-chinese-students-are-a-potential-threat)that FBI Director Christopher Wray discussed the counterintelligence threat of Chinese nationals in the U.S. academic sector during a Senate Intelligence Committee hearing.

"There are certain policies and actions by our government that, while directed at foreign nationals, could affect Americans who happen to be of certain ethnicities. In this case, tarring Chinese foreign national students en masse as being more suspicious is overbroad and will also feed into the false and harmful narrative that somehow Chinese-Americans are more suspicious. It is this false narrative that contributed to the wrongful indictments of Chinese-Americans like Sherry Chen and Professor Xiaoxing Xi. I worked on those cases last year and helped cause the Department of Justice to change its policies to help make sure Chinese-Americans are not targeted by law enforcement because of their ethnicity.

I called on FBI Director Wray to clarify his comments and make a strong statement that Chinese-Americans are not viewed by the FBI as any more suspicious than any other American.

I also have a suggestion for the Trump Administration. Before spending a lot of time and resources looking at foreign nationals allegedly getting publicly available information, perhaps the Administration should first crack down on the over 130 Americans in the White House who still don't have permanent security clearances and are inappropriately viewing highly classified non-public information."

###

The Prosecution Unravels: The Case of Wen Ho Lee

By Matthew Purdy With James Sterngold

Feb. 5, 2001

See the article in its original context from
February 5, 2001, Section A, Page 1 Buy Reprints

VIEW ON TIMESMACHINE

TimesMachine is an exclusive benefit for home
delivery and digital subscribers.

In a secure warren of the Los Alamos weapons laboratory, investigators mined the office of Wen Ho Lee. Books, reports, notes written in Chinese -- everything was handled with latex gloves to preserve the evidence. Just days before, laboratory officials had fired the computer scientist for security violations, and investigators suspected he was a spy, but the search was yielding little. Then agents discovered the list.

It was on his desk, a record of computer files containing highly sensitive weapons-design information. With the help of a Los Alamos physicist, investigators determined that Dr. Lee had downloaded the secret files from the laboratory's classified computer system and transferred them to computer tapes. Some of the tapes were missing. The potential compromise of America's nuclear weapons secrets was staggering.

"It's unimaginable," the physicist, John Romero, remembers thinking.

For three years, agents had suspected Dr. Lee of giving China information on America's most sophisticated nuclear warhead, the W-88. But their meandering espionage investigation had been short on resources and long on missed opportunities. The discovery of the download, in late March 1999, was the first hard evidence of any crime -- the key, perhaps, to the maddening enigma of Wen Ho Lee. Now, with the case out in the open and hotly debated, and Dr. Lee's huge security breach raising the stakes of the investigation, the government, in the words of one F.B.I. official, "sent in the cavalry."

Agents conducted 1,000 interviews over nine months, scouring the globe for evidence that Dr. Lee had leaked his secrets. The Federal Bureau of Investigation carried out its largest computer forensic investigation ever. Investigators traced years of Dr. Lee's telephone calls. Prosecutors pressed him to explain himself, and when he did not, they brought a 59-count indictment and convinced a federal judge that he was so dangerous he had to be jailed without bail. He spent nine months in such restrictive conditions that he was shackled during recreation.

In the field and then in the courtroom, the prosecution of Wen Ho Lee was a final attempt to understand a man whose deepening suspiciousness had taunted the government for nearly 20 years. When they failed to uncover espionage, prosecutors constructed an unusual and risky strategy, seeking to put him in prison for life on charges they had no direct evidence to support. It was a leap, and in the end, it fell short.

Last September, the judge freed Dr. Lee, declaring that his jailing had "embarrassed our entire nation and each of us who is a citizen of it." The Justice Department wound up with a public relations disaster and a guilty plea to the crime it had evidence of from the start -- a single felony count of mishandling national security information.

Dr. Lee, 61, had always left investigators feeling that he was hiding something. He had a history of deceiving the authorities about security matters and clandestine contact with foreign scientists. Now, agents discovered that he had tried to delete his downloaded files as they closed in on him. After he was kicked out of the bomb-design area of Los Alamos for security violations, he found ways to sneak back in. Investigators also began seeing signs that he might be exploring a relationship with a military research institute in his native Taiwan.

Whatever the evidence of deception, though, the prosecution's most powerful charges unraveled as defense lawyers homed in on gaps in the case. Without proof that Dr. Lee was a spy, prosecutors charged him with intent to injure the United States and help a foreign country. But they were never sure why he had taken the secrets, or which country he might have planned to help with them.

They initially suspected he was a spy for China. Then they toyed with China's nemesis, the regime on Taiwan. Finally, in court last summer, they presented a menu of surprising possibilities that included Australia and Switzerland. And they said they believed his motive for downloading the information was to enhance his job prospects. To the judge who had ordered him jailed, and to Dr. Lee's increasingly vocal supporters, the government's cold, hard case was melting away.

Another blow came from John L. Richter, an esteemed weapons designer who had played a crucial role in beginning the espionage investigation that ensnared Dr. Lee. Testifying in court, Dr. Richter played down the threat of Dr. Lee's crime. Although he later backed away from that assessment, Dr. Richter said he had spoken out in court because he believed Dr. Lee "had suffered enough" and should be set free.

In one sense, prosecutors got what they wanted -- the felony plea and an agreement from Dr. Lee to tell all under oath. But, to this day, they remain taunted by what they do not know. The debriefings over the last few months and further investigation have left them with a blur of questions. Unsatisfied with some of his explanations, investigators are still exploring his dealings with Taiwanese and Chinese scientists.

As for the downloading itself, frustrated investigators are left with nothing but Dr. Lee's innocent explanation: He downloaded the information to protect his work and tossed the tapes that are missing in a trash bin behind his office at Los Alamos. They have never been found.

At the F.B.I., a top official voiced the bureau's latest conclusion: "I don't think anyone fully understands Wen Ho Lee."

KEEPING WATCH

Each step of the F.B.I. investigation seemed to fuel old suspicions and cast new doubt.

Day and night throughout 1999, agents sat in cars outside Wen Ho Lee's red ranch house on Barcelona Avenue near Los Alamos, N.M., where suburban development abuts striking mesas. They trailed him everywhere, and he could hardly have appeared more harmless and cordial. He told his neighbor, Jean Marshall, that the agents especially liked it when he went fishing because it gave them a chance to get out of their hot cars. Once, when he had to travel out of town, he changed his schedule to accommodate his watchers.

But as investigators pieced together Dr. Lee's past, their already dim view of him darkened.

Their computer investigation showed that in early 1999, just as agents were pressing him for evidence of espionage, Dr. Lee had been busily trying to delete the downloaded files. On Feb. 10, for example, after failing an F.B.I. polygraph, Dr. Lee deleted 310 files, F.B.I. documents show.

Investigators also discovered that he had continued to sneak into the bomb-design area, X Division, after his access was canceled. In January of 1999, soon after losing his access, he was let in by an unwitting security officer. Other times he simply walked in behind division

employees, lawyers knowledgeable about the case said. (In his recent debriefing, Dr. Lee told investigators that he had slipped in through an open door just hours after he was barred from X Division, the lawyers said.)

"Each day we found more information that cast doubt on him," said David V. Kitchen, then head of the F.B.I.'s Albuquerque office. In January, Mr. Kitchen had recommended closing the espionage investigation of Dr. Lee, because he appeared cooperative and had innocent explanations for everything. Since the discovery of the download, everything had begun to look less innocent.

In August 1998, agents ran a sting operation to see if Dr. Lee would bite at the chance to meet with an agent posing as a Chinese intelligence agent. Dr. Lee's reaction appeared ambiguous to investigators.

When the agent called, Dr. Lee said there was a laboratory policy against meeting foreign representatives without approval. However, according to a secret F.B.I. report recently obtained by The New York Times, "Lee indicated that it is all right to talk on the phone since everything Lee has done was in the open." Dr. Lee first agreed to meet the agent, then called back to say he could not. When the agent called back the next day, Dr. Lee agreed to take his beeper number.

"He doesn't take the bait," said one former government official, "but he seems to be feeling him out."

He also seemed to be feeling Taiwan out. In March and April of 1998, according to court testimony, Dr. Lee had spent six weeks in Taiwan as a consultant to the Chung Shan Institute, a government defense complex where American officials say Taiwan has done nuclear weapons research. Dr. Lee's trip was taken with the approval of laboratory officials.

Investigators discovered that while on that trip, Dr. Lee called the Los Alamos computer help desk to find out if he could access his classified computer. He was told he could not, but investigators later found that he had downloaded an unclassified computer code from Los Alamos to his computer in Taiwan.

Those dealings with Taiwan echoed the F.B.I.'s first contact with Dr. Lee in the early 1980's. Dr. Lee had been picked up on a wiretap, offering to help a fellow scientist who was under investigation for spying. In interviews at the time, Dr. Lee admitted to agents that he had improperly passed unclassified but restricted scientific information to Taiwanese officials.

If the investigation of the download was fueling the same old suspicions about Dr. Lee, investigators were getting the same old result.

Agents determined that 9 of 15 computer tapes Dr. Lee had made were missing, but their exhaustive search -- they even visited every private storage facility in New Mexico -- left them unable to refute Dr. Lee's explanation that he had destroyed them. They spent months searching the Los Alamos computer system, even shutting it down entirely for three weeks, but found no evidence that anyone had gotten into Dr. Lee's computer files. They did discover that Dr. Lee had given his password to his children so they could connect to the Internet and play computer games through his Los Alamos computer while they were at college.

And they had no evidence to counter Dr. Lee's only public explanation -- in a "60 Minutes" interview in August 1999 -- that he had downloaded and copied the information so he would have backup files for his work.

Investigators began to see hints of another motive. F.B.I. agents traveled to Taiwan and found that in addition to lecturing and consulting there in 1998, he also met with a company to explore job opportunities, federal investigators testified in court.

Agents discovered more evidence of Dr. Lee's job hunting when they searched his house in April 1999 -- seven letters to scientific institutes and universities around the world inquiring about job prospects. Dr. Lee wrote them in 1993 and 1994, after he had learned he was on a list of employees to be laid off in the event of a budget crunch.

The downloading that Dr. Lee eventually was charged with occurred during that same period, even though investigators discovered that he had actually begun transferring some material as early as 1988, well before his job was threatened.

Perhaps, investigators thought, the download was an insurance policy. Perhaps, entering his late 50's and contemplating retirement at 60, he figured that the secrets of Los Alamos would make him more marketable.

"We may not be able to show he was a spy," said one F.B.I. official, "but we can show he was not just a wayward scientist."

SECRETS AND SCIENCE

The government had no evidence of espionage. So it fashioned an unusual prosecution strategy based on the idea that Dr. Lee must have intended to injure the United States.

In April 1999, federal prosecutors from Albuquerque went up the mountain to Los Alamos, where scientists gave them what one lawyer called the " 'Oh, my God' speech." Having assessed Dr. Lee's security breach, the scientists told prosecutors, "There was nothing more valuable that anyone could take."

Computer forensic investigators re-created Dr. Lee's deleted files and determined that Dr. Lee had moved 806 megabytes of information (the equivalent of papers stacked 134 feet high, they said) that contained the tools for computer-simulated weapons testing, a valuable commodity in an age of nuclear test bans.

The files included computer codes, which he had helped write, that used the information from decades of actual weapons tests to simulate the detonation of bombs. He also downloaded files containing sketches and dimensions of weapons and files giving physical properties of bombs.

Experts would later testify that while the files alone would not allow someone to replicate a weapon, in knowledgeable hands they could advance a nuclear weapons program. And officials had another fear, one they were prohibited for security reasons from voicing publicly: Dr. Lee's files contained information about currently deployed weapons, which could help an enemy defend against them.

The task of translating the science into a criminal case fell to Robert J. Gorence, the first assistant to John Kelly, the United States attorney for New Mexico.

At 41, Mr. Gorence had wide experience as a prosecutor -- drug cases on Indian reservations, complicated savings and loan trials, the pursuit of the runaway spy Edward Lee Howard. Intense and aggressive, Mr. Gorence threw himself into the Lee case, spending weeks at Los Alamos with other investigators, interviewing scientists and reading physics texts. Steeped in the details, he could rattle off such obscure facts as the amount of time it takes for an atom bomb to "go critical." (Fifty millionths of a second.)

At one point, Mr. Gorence went to Kirtland Air Force base in Albuquerque, where the government stores films of nuclear weapons tests in a secure vault, chilled to preserve the pictures. Impressed by the films' awful drama, he told colleagues he wanted to show them to a jury to demonstrate the power of the secrets Dr. Lee had compromised.

Even so, evidence of a crime beyond the security breach itself was limited. As Mr. Kitchen, the former F.B.I. official, put it, "Short of espionage, what do we have?"

Mr. Gorence consulted the Atomic Energy Act, which he had read a few years earlier in preparation for the threat of protests at Los Alamos on the 50th anniversary of the Japan bombings. He focused on the only two provisions in American law that allow life sentences for mishandling secrets even without proof of espionage, seemingly a perfect fit for Wen Ho Lee.

No one had ever been prosecuted under those statutes, according to court testimony, and proving the charges, one prosecutor acknowledged, was "hardly a slam dunk." But federal officials all the way up to the attorney general, Janet Reno, signed on to the charges, which

accused Dr. Lee of acting with "intent to injure the United States, and with the intent to secure an advantage to a foreign nation."

Prosecutors had no hard evidence that he planned to give away the secrets, but they reasoned that the simple absence of an innocent explanation showed his criminal intent. They emphasized the deliberate nature of the download -- they estimated it had taken him 40 hours over 70 days. And they argued that his long experience at Los Alamos and secretive manner showed he knew what he was doing was wrong. In fact, after the download was discovered, he at first denied making the tapes, according to Congressional testimony.

They argued further that his actions injured the United States by denying it exclusive possession of the secrets, and they began lining up Pentagon officers to testify about the potential effect on American military strategy. Proving that Dr. Lee had aided another nation was more difficult, but prosecutors argued that they did not have to prove he had a specific country in mind when downloading the material, only that he eventually intended to help one.

The strength of the prosecution's case, one Justice Department official said, lay in the sheer "depth and scope" of the material. But that was also a major potential pitfall.

Many cases involving classified information are not brought to trial for fear of divulging secrets. In the Lee case, top government officials, including the attorney general, the director of central intelligence and the national security adviser, met at the White House on a Saturday in December 1999 to discuss the risk of prosecution. They decided the case had to go forward, lest Dr. Lee's tapes be passed to a foreign country, since efforts to strike a deal had failed. One letter from Mr. Kelly, the United States attorney, to defense lawyers ended in blunt frustration: "In short, we want you to tell us why he made the tapes!"

If they ended up having to go to trial, the officials decided, they would try to thread a needle on the secrets issue, allowing only summaries of the data on Dr. Lee's files to be used.

Still, as Mr. Kelly conceded in an interview, "no one wanted to go to trial." And bringing powerful charges, another government lawyer said, was partly a strategy to get information from Dr. Lee, and perhaps force a plea.

The indictment, handed up Dec. 10, made no mention of the W-88 or of spying. But in bail hearings, prosecutors presented a dark image of Dr. Lee by sweeping together all they knew about him -- from his earliest suspicious contacts with foreign scientists to his attempts to delete his downloaded files.

At the first bail hearing, Stephen M. Younger, the associate director for nuclear weapons at Los Alamos, said the information on the missing tapes could "in the wrong hands, change the global strategic balance."

A magistrate denied bail and two weeks later, after Dr. Lee appealed, prosecutors raised the ante before Judge James A. Parker of Federal District Court. "This court, I believe, faces a you-bet-your-country decision," Paul Robinson, president of the Sandia National Laboratories, told the judge.

The judge indicated he was leaning toward a restrictive form of house arrest, but in a secret hearing the prosecution warned of dire circumstances.

Dr. Lee could be "snatched and taken out of the country" by a hostile element looking for the missing tapes, Mr. Kelly said, according to a transcript of the hearing.

Robert Messemer, the F.B.I. agent brought in as the lead investigator because of his background in espionage cases and proficiency in Chinese, was more pointed.

"We anticipate a marked increase in hostile intelligence service activities both here in New Mexico and throughout the United States in an effort to locate those tapes," he said. "Our surveillance personnel do not carry firearms, and they will be placed in harm's way if you require us to maintain this impossible task of protecting Dr. Lee."

SOLITARY CONFINEMENT

Jailed for nine months, Dr. Lee found release in music, literature and science.

Wen Ho Lee was held in solitary confinement for nine months at the Santa Fe County Detention Facility. He was kept in his cell 23 hours a day. A small light burned constantly so guards could watch him at all hours. He was allowed to see his family just one hour a week, and they had to speak English -- not Mandarin, which they speak at home -- so the F.B.I. could listen. And like other prisoners in solitary confinement, he was shackled whenever he left his cell, even while exercising or meeting with his lawyers.

Early last January, when Dr. Lee's lawyers demanded that his conditions be eased, prosecutors responded that Ms. Reno had personally approved them.

"These special administrative measures were requested for one reason and one reason only: to restrict Dr. Lee's ability to pass information through intermediaries that could have the devastating consequence of disseminating the nuclear secrets he had stolen from Los Alamos," Ms. Reno later told a Senate hearing.

Eventually, the government loosened its restrictions. Officials arranged for a Mandarin-speaking agent so Dr. Lee could talk to his family in his native language. They gave him a radio and removed his chains during exercise.

But if the government hoped Dr. Lee would crack, he displayed hardly a fissure.

Dr. Lee is a meticulous man, obsessively neat and ordered. In a recent picture-taking session at his home, Dr. Lee led a visitor to a small room that his daughter, Alberta, called "his room." It was impeccably clean and sparsely furnished -- a bed, a desk with a few books, an amplifier, turntable and speakers and Dr. Lee's collection of classical and opera records, stacked neatly on shelves. His daughter said he would stay there for hours, listening to music. In the garage, Dr. Lee's used but clean gardening tools were laid neatly on a shelf. Later, cooking dinner, he moved with methodical precision, chopping, arranging food in piles and cleaning the cooking area before sitting down to eat with guests.

In prison, he re-created his world. He listened to classical music on the radio. He read novels. He wrote large parts of a mathematics textbook. A friend, Cecilia Chang, recalls him saying that while physically he was in prison for nine months, "spiritually, I lived with my music and my literature and my science."

The government's case had created a storm, but, once again, the man at the center seemed curiously unchanged. When a jail monitor visited him, a federal official later told Congress, Dr. Lee said that, other than his freedom, his only wish was for "additional fruit at the evening meal."

FIGHTING BACK

The defense knew it had to fight two battles: one in court, the other in the public arena.

The defense lawyers were not as serene as their client. Their man was in prison. The public seemed convinced he was a spy for China. And the government was throwing heavy resources at the case.

The lead lawyer was Mark Holscher, then 36, a white-collar criminal specialist at the Los Angeles law firm of O'Melveny & Myers. A former federal prosecutor, he had made his reputation, in part, prosecuting Heidi Fleiss, known as the Hollywood Madam. Mr. Holscher agreed to take the Lee case pro bono after being found by Dr. Lee's daughter.

The second lawyer, John D. Cline, had handled the classified material issues for Oliver North's defense in the Iran-Contra prosecution. As time wore on, and donations to the defense increased, more lawyers were added.

They saw two battles, Mr. Holscher said, "one in the court and the other in the public at large." They fought on both fronts.

The government provided the defense with a secure room on the top floor of the imposing federal courthouse in Albuquerque where they could prepare their case and meet with their client under the eye of a security camera.

The first crack in the prosecution appeared as they sifted through testimony from the December bail hearing. A Los Alamos computer expert had testified that the downloaded files were classified under a category called PARD, "protect as restricted data" -- a rule for handling computer-generated material that includes some secrets in a sea of more ordinary information.

Defense lawyers recognized that meant that the files themselves were not classified "top secret" or "secret." It was a perfect opportunity to strike at the heart of the government's claim that the files represented the nation's "crown jewels." Prosecutors acknowledge that they had not been fully aware of the PARD issue. While there was still little question Dr. Lee had downloaded important secrets, they knew the defense would press the issue with a jury.

The defense found its next opening by asking prosecutors one simple question: Which country did they expect to argue Dr. Lee was intending to aid? Defense attorneys expected the answer to reveal the murky center of the government's most powerful allegations, but even they were surprised by the results.

Mr. Gorence resisted answering, arguing that the government was under no obligation to say. But by the spring of 1999, Mr. Gorence was no longer the lead prosecutor on the case. Mr. Kelly had left his post to run for Congress. Officials in Washington not only declined to appoint Mr. Gorence as United States attorney but also, without any public explanation, brought in a new prosecutor.

He was George A. Stamboulidis, a federal prosecutor on Long Island who had long experience with organized crime and other complex cases. Fresh on the Lee case, he made his first substantive move.

Under orders from Judge Parker, Mr. Stamboulidis answered the defense's question. He filed a document listing Australia, France, Germany, Hong Kong, Singapore, Switzerland and Taiwan -- the countries on the job search letters found in Dr. Lee's house. Mr. Stamboulidis also threw in China.

Defense lawyers had believed that the government's suspicions of Dr. Lee as a spy for China had waned. Indeed, under Mr. Gorence, the government was building a case that Dr. Lee might have been aiding Taiwan. But Australia and Switzerland?

"These are not countries which anyone other than the prosecutors have identified as presenting any kind of nuclear threat to the United States," Mr. Holscher said, snickering.

Judge Parker had a more sober, but equally damaging, view. Writing later in a decision releasing Dr. Lee, he said, "Enhancing one's resume is less sinister than the treacherous motive the government, at least by implication, ascribed to Dr. Lee at the end of last year."

Defense lawyers began another assault in July, announcing in a secret hearing that they intended to bring a nuclear bomb to court. Not a real bomb, but something just as audacious -- an actual bomb blueprint.

One of the government's constant refrains had been that Dr. Lee had stolen "electronic blueprints" for nuclear weapons. Therefore, the defense argued, it had the right to rebut that by introducing a real blueprint. The defense knew the government would resist, and hoped that might persuade the judge to drop the charges on fair-trial grounds.

This was a preview of the defense's strategy on secrets. Using the classified material, Mr. Cline said at the closed hearing, would be necessary for proving four central defense arguments: that most of the downloaded material was already in the public domain; that some of the computer codes contained flaws that made them less useful; that the codes were related to Dr. Lee's work; and that they were difficult to use without user manuals, which were not on the tapes.

The case ended before Judge Parker could decide whether to allow the use of the bomb blueprints or other secrets at a trial. But based on early rulings that some secrets might be relevant to the defense, Ms. Reno testified later, prosecutors expected to be forced to cross "an exposure threshold we had already determined posed an unacceptable risk."

QUESTIONS OF FAIRNESS

Accusations of racial profiling and overzealous prosecution helped turn the case in Dr. Lee's favor.

As much as anything, what ultimately undid the prosecution were questions of fairness. The image of the diminutive Wen Ho Lee -- still untried, not even charged with espionage -- chained in a cocoon of silence, transformed him in the public eye from villain to victim.

Asian-American groups, energized by the case, charged that Dr. Lee was a victim of racial profiling, unfairly singled out for prosecution. Scientific and civil rights groups joined in. The clearest, loudest voice belonged to Alberta Lee, a 26-year-old technical writer who gave speech after speech hammering away at a message defense lawyers were arguing in court.

A defense motion claiming selective prosecution contrasted Dr. Lee's treatment with that of John M. Deutch, the former director of central intelligence, whom the Justice Department initially declined to prosecute for keeping national security secrets on his home computer.

(The department eventually opened an investigation, but Mr. Deutch was among those pardoned by Bill Clinton on his last day as president.)

Defense lawyers made sure their legal papers got to reporters. One document that particularly resonated was a declaration from Robert Vrooman, former head of counterintelligence at Los Alamos, stating that a major reason investigators initially suspected Dr. Lee had spied for China was because he was ethnic Chinese.

Indeed, Dr. Lee's race was one strand of investigators' suspicion. In an affidavit seeking permission to search Dr. Lee's house in April 1999, an F.B.I. agent stated that Chinese "intelligence operations virtually always target overseas ethnic Chinese with access to intelligence information."

But Mr. Vrooman knew there was more to investigators' suspicions. Mr. Vrooman himself had raised concerns about Dr. Lee's contacts with Chinese scientists in the late 1980's and had identified Dr. Lee to Energy Department investigators as a potential suspect in the W-88 case. Beyond that, Mr. Vrooman was one of three laboratory officials reprimanded for the handling of the Lee case, and his critics said that gave him a motive to criticize the investigation.

Even so, supporters of Dr. Lee saw Mr. Vrooman's declaration as further evidence of overzealous prosecution. Their view was bolstered at a new bail hearing in August, ordered by Judge Parker.

In testimony, Mr. Messemer, the lead F.B.I. agent, acknowledged having misstated important evidence against Dr. Lee. For example, Mr. Messemer had testified in December 1999 that Dr. Lee had lied by asking a colleague to borrow his computer to download a resume. In fact, Dr. Lee was downloading nuclear secrets, and that testimony seemed to show Dr. Lee's deception -- an element in proving the intent charges.

But defense lawyers discovered that the colleague, in interviews with the F.B.I., had never said Dr. Lee told him he was downloading a resume. Mr. Messemer told the judge he had made "an honest error," and never intended "to mislead you or anyone in this court or any court." Next he acknowledged that after further investigation, there was no evidence that the job-search letters found in Dr. Lee's house had been sent. That undercut the prosecution's image of Dr. Lee feverishly job-hunting.

If Dr. Lee needed one more nudge to turn the case in his favor, it was delivered by John L. Richter. A plain-talking Texan and veteran bomb designer, Dr. Richter was making his second pivotal appearance in the Lee case.

In 1995, he was the first to suggest that the Chinese might have significant information about the W-88 warhead. Even though he eventually backed off that opinion, it helped start the investigation that led to the discovery of Dr. Lee's download and his jailing.

Now, asked about the danger of Dr. Lee's tapes falling into enemy hands, Dr. Richter responded: "I think that keeping him locked up the way he is is much more injurious to the reputation of the United States. And that is one reason that I am here."

Without having reviewed the downloaded information, he minimized its importance, saying "99 percent of it was unclassified in the open literature."

In a subsequent interview and Congressional testimony, Dr. Richter said his "99 percent" statement referred only to the basic physics underlying the computer codes. But he said other elements of the files did hold important secrets.

Dr. Richter had seen the testimony of laboratory officials that helped jail Dr. Lee as hyperbole. Having played a role in starting the Lee affair, he now thought it was time to end it.

"If I had any influence in getting him out," he said recently, "I figured that's a payback."

APOLOGY FROM THE BENCH

After pleading guilty to one charge, Dr. Lee was free. The judge said he had been 'induced' to jail Dr. Lee.

On Aug. 24, 2000, Judge Parker issued a brief order saying he had decided to release Dr. Lee under stringent conditions.

Just days before, Mr. Stamboulidis had warned that the risk of freeing Dr. Lee was "of a caliber where hundreds of millions of people could be killed." But after the judge's order, prosecutors began trying to cut a plea deal. By early September, they had one.

Dr. Lee agreed to plead guilty to one felony count of illegally gathering and retaining national security data. He did not admit to intending to harm the United States or aid a foreign country. He agreed to a sentence of time served, with no probation, and to undergo 60 hours of debriefing, under oath, by the government.

Dr. Lee had one last surprise before entering the guilty plea. Asked for the first time by the government, he acknowledged having made copies of the tapes. It made prosecutors suspicious all over again, but they went ahead.

On Wednesday, Sept. 13, Dr. Lee stood in court and admitted his guilt. But the drama of the day was Judge Parker's soliloquy.

"What I believe remains unanswered," he said, "is the question, What was the government's motive in insisting on your being jailed pretrial under extraordinarily onerous conditions of confinement until today, when the executive branch agrees that you may be set free essentially unrestricted? This makes no sense to me.

"A corollary question, I guess, is, Why were you charged with the many Atomic Energy Act counts for which the penalty is life imprisonment, all of which the executive branch has now moved to dismiss and which I just dismissed?"

The judge blamed Clinton administration decision makers, saying, "I was induced" to jail Dr. Lee before his trial. But it had become clear that "it was not necessary."

He ended, "I sincerely apologize to you, Dr. Lee, for the unfair manner you were held in custody by the executive branch."

EPILOGUE

Even now, the case is not quite over. Agents continue to look at some of Dr. Lee's activities, and the W-88 mystery remains unsolved.

The government's debriefing of Dr. Lee ended late last year. He acknowledged making as many as a dozen trips to Taiwan over the last two decades -- more than officials previously knew about -- although it remains unclear how many were for purely personal reasons.

According to people knowledgeable about the case, investigators are looking at aspects of two of those trips, taken in 1998 with full knowledge of laboratory officials. One was his six-week visit to the Chung Shan military institute, where he received a consulting fee of about $5,000; the second was paid for by a private company in Taiwan. Investigators are also interested in small family accounts in Taiwanese and Canadian banks.

And they are continuing to examine Dr. Lee's relationships with Chinese scientists, including a dinner he held for one scientist where officials say they have information that a computer code might have been discussed.

Mr. Holscher, Dr. Lee's lawyer, called any suggestion of wrongdoing false, adding, "even more disappointing is that anonymous government officials risk violating federal criminal law by talking about the investigation."

Under the plea agreement, prosecutors have the option of submitting Dr. Lee to another lie detector test.

As for the missing computer tapes, they were not found in a thorough search of the Los Alamos landfill.

Dr. Lee is getting a curtain call. He recently agreed to tell his story. This time it will not be under oath. He has a contract for a book and mini-series.

Notra Trulock, who began the W-88 investigation as the intelligence director at the Energy Department, is now the spokesman for the Free Congress Foundation, a conservative research group in Washington. He has a contract for a book that he is thinking of calling "Kindred Spirit: The Inside Story of the Chinese Espionage Scandal."

After Dr. Lee's release, President Bill Clinton rebuked his own Justice Department, saying, "I always had reservations about the claims that were made denying him bail." He added, "The whole thing was quite troubling to me."

The W-88 investigation itself is stalled. Just as the downloading case was gathering steam in the summer of 1999, the F.B.I. was coming to grips with the flaws of its initial inquiry.

After interviewing scientists who had conducted an analysis for the Energy Department in 1995, F.B.I. officials determined that many of them had disagreed with the conclusion that China, using stolen secrets, had built a weapon like the W-88.

At the same time, a White House panel pointed out that the stolen information about the W-88 could have come not just from Los Alamos but from numerous energy and defense installations as well as private contractors. And intelligence experts say they have no evidence that China has actually deployed any long-range weapons that incorporate the lost secrets, though they believe a new generation of weapons may do so by 2015.

In September 1999, Attorney General Janet Reno and Louis J. Freeh, the F.B.I. director, ordered federal agents to broaden their spy investigation. But the new trail proved so cold and so wide open that investigators made little headway. "You're looking at potentially thousands of points of compromise," a senior federal official said, "so it becomes an undoable problem."

Neil J. Gallagher, the bureau's national security chief, said in a recent interview that if the bureau had known in the beginning what it learned, it would not have been so quick to focus on Wen Ho Lee. He said he would have labeled the investigation the "potential" compromise of the W-88.

The chief suspect, he said, "would have been unknown."

Under Suspicion

After Wen Ho Lee was freed from jail last September, a furor erupted over how the government had handled the case and how the press, especially The New York Times, had covered it. Several weeks later, The Times published an unusual statement assessing its

coverage. It found many strengths, but also some weaknesses. In the statement, the paper promised a thorough re-examination of the case. After more than four months of reporting, the result is this two-part series that began yesterday.

MIT News
ON CAMPUS AND AROUND THE WORLD

Letter to the MIT community: Immigration is a kind of oxygen

MIT News Office
June 25, 2019

The following email was sent today to the MIT community by President L. Rafael Reif.

To the members of the MIT community,

MIT has flourished, like the United States itself, because it has been a magnet for the world's finest talent, a global laboratory where people from every culture and background inspire each other and invent the future, together.

Today, I feel compelled to share my dismay about some circumstances painfully relevant to our fellow MIT community members of Chinese descent. And I believe that because we treasure them as friends and colleagues, their situation and its larger national context should concern us all.

The situation

As the US and China have struggled with rising tensions, the US government has raised serious concerns about incidents of alleged academic espionage conducted by individuals through what is widely understood as a systematic effort of the Chinese government to acquire high-tech IP.

PRESS MENTIONS

Carey Goldberg reports for WBUR *CommonHealth* on the MIT president's recent letter to the community describing immigration as a kind of oxygen. "In his letter, MIT President Reif adds the force of his own bully pulpit, writing that MIT flourishes because it draws talent from around the globe," writes Goldberg.

90.9wbur

RELATED

President L. Rafael Reif

ARCHIVES

3 Questions: Richard Lester on the MIT China Summit

For great challenges, a global strategy

As head of an institute that includes MIT Lincoln Laboratory, I could not take national security more seriously. I am well aware of the risks of academic espionage, and MIT has established prudent policies to protect against such breaches.

But in managing these risks, we must take great care not to create a toxic atmosphere of unfounded suspicion and fear. Looking at cases across the nation, small numbers of researchers of Chinese background may indeed have acted in bad faith, but they are the exception and very far from the rule. Yet faculty members, post-docs, research staff and students tell me that, in their dealings with government agencies, they now feel unfairly scrutinized, stigmatized and on edge – because of their Chinese ethnicity alone.

Nothing could be further from – or more corrosive to – our community's collaborative strength and open-hearted ideals. To hear such reports from Chinese and Chinese-American colleagues is heartbreaking. As scholars, teachers, mentors, inventors and entrepreneurs, they have been not only exemplary members of our community but exceptional contributors to American society. I am deeply troubled that they feel themselves repaid with generalized mistrust and disrespect.

The signal to the world

For those of us who know firsthand the immense value of MIT's global community and of the free flow of scientific ideas, it is important to understand the distress of these colleagues as part of an increasingly loud signal the US is sending to the world.

Protracted visa delays. Harsh rhetoric against most immigrants and a range of other groups, because of religion, race, ethnicity or national origin. Together, such actions and policies have turned the volume all the way up on the message that the US is closing the door – that we no longer seek to be a magnet for the world's most driven and creative individuals. I believe this message is not consistent with how America has succeeded. I am certain it is not how the Institute has succeeded. And we should expect it to have serious long-term costs for the nation and for MIT.

For the record, let me say with warmth and enthusiasm to every member of MIT's intensely global community: We are glad, proud and fortunate to have you with us! To our alumni around the world: We remain one community, united by our shared values and ideals! And to all the rising talent out there: If you are passionate about making a better world, and if you dream of joining our community, we welcome your creativity, we welcome your unstoppable energy and aspiration – and we hope you can find a way to join us.

* * *

In May, the world lost a brilliant creative force: architect I.M. Pei, MIT Class of 1940. Raised in Shanghai and Hong Kong, he came to the United States at 17 to seek an education. He left a legacy of iconic buildings from Boston to Paris and China to Washington, DC, as well on our own campus. By his own account, he consciously stayed alive to his Chinese roots all his life. Yet, when he died at the age of 102, the *Boston Globe* described him as "the most prominent American architect of his generation."

Thanks to the inspired American system that also made room for me as an immigrant, *all of those facts can be true at the same time*.

As I have discovered through 40 years in academia, the hidden strength of a university is that every fall, it is refreshed by a new tide of students. I am equally convinced that part of the genius of America is that it is continually refreshed by immigration – by the passionate energy, audacity, ingenuity and drive of people hungry for a better life.

There is certainly room for a wide range of serious positions on the actions necessary to ensure our national security and to manage and improve our nation's immigration system. But above the noise of the current moment, the signal I believe we should be sending, loud and clear, is that the story of American immigration is essential to understanding how the US became, and remains, optimistic, open-minded, innovative and prosperous – a story of never-ending renewal.

In a nation like ours, immigration is a kind of oxygen, each fresh wave reenergizing the body as a whole. As a society, when we offer immigrants the gift of opportunity, we receive in return vital fuel for our shared future. I trust that this wisdom will always guide us in the life and work of MIT. And I hope it can continue to guide our nation.

Sincerely,

L. Rafael Reif

Topics: **Staff** **President L. Rafael Reif** **Administration** **Immigration** **China** **Faculty** **Students**

About This Website

This Website is maintained by the MIT News Office, part of the Office of Communications.

MIT News Office • Building 11-400
Massachusetts Institute of Technology • Cambridge, MA 02139-4307

The New York Times

Statement by Judge in Los Alamos Case, With Apology for Abuse of Power

Sept. 14, 2000

See the article in its original context from
September 14, 2000, Section A, Page 25 Buy Reprints

VIEW ON TIMESMACHINE

TimesMachine is an exclusive benefit for home
delivery and digital subscribers.

Following is a transcript of a statement yesterday by Judge James A. Parker of Federal District Court in Albuquerque to Dr. Wen Ho Lee, who pleaded guilty to mishandling nuclear secrets, as recorded by the court reporter. At one point the federal prosecutor in the case, George Stamboulidis, defended his dealings with the defense lawyer Mark Holscher:

JUDGE PARKER -- Dr. Lee, you have pled guilty to a serious crime. It's a felony offense. For that you deserved to be punished. In my opinion, you have been punished harshly, both by the severe conditions of pretrial confinement and by the fact that you have lost valuable rights as a citizen.

Under the laws of our country, a person charged in federal court with commission of a crime normally is entitled to be released from jail until that person is tried and convicted. Congress expressed in the Bail Reform Act its distinct preference for pretrial release from jail and prescribed that release on conditions be denied to a person charged with a crime only in exceptional circumstances.

The executive branch of the United States government has until today actually, or just recently, vigorously opposed your release from jail, even under what I had previously described as draconian conditions of release.

During December 1999, the then-United States attorney, who has since resigned, and his assistants presented me, during the three-day hearing between Christmas and New Year's Day, with information that was so extreme it convinced me that releasing you, even under

the most stringent of conditions, would be a danger to the safety of this nation. The then-United States attorney personally argued vehemently against your release and ultimately persuaded me not to release you.

In my opinion and order that was entered Dec. 30, 1999, I stated the following: "With a great deal of concern about the conditions under which Dr. Lee is presently being held in custody, which is in solitary confinement all but one hour of the week, when he is permitted to visited his family, the court finds, based on the record before it, that the government has shown by clear and convincing evidence that there is no combination of conditions of release that would reasonably assure the safety of any other person and the community or the nation."

After stating that in the opinion, I made this request in the opinion right at the end: "Although the court concludes that Dr. Lee must remain in custody, the court urges the government attorneys to explore ways to lessen the severe restrictions currently imposed upon Dr. Lee while preserving the security of sensitive information."

I was very disappointed that my request was not promptly heeded by the government attorneys.

After December, your lawyers developed information that was not available to you or them during December. And I ordered the executive branch of the government to provide additional information that I reviewed, a lot of which you and your attorneys have not seen.

With more complete, balanced information before me, I felt the picture had changed significantly from that painted by the government during the December hearing. Hence, after the August hearing, I ordered your release despite the continued argument by the executive branch, through its government attorneys, that your release still presented an unacceptable extreme danger.

I find it most perplexing, although appropriate, that the executive branch today has suddenly agreed to your release without any significant conditions or restrictions whatsoever on your activities. I note that this has occurred shortly before the executive branch was to have produced, for my review in camera, a large volume of information that I previously ordered it to produce.

From the beginning, the focus of this case was on your motive or intent in taking the information from the secure computers and eventually downloading it on to tapes. There was never really any dispute about your having done that, only about why you did it.

What I believe remains unanswered is the question: What was the government's motive in insisting on your being jailed pretrial under extraordinarily onerous conditions of confinement until today, when the executive branch agrees that you may be set free

essentially unrestricted? This makes no sense to me.

A corollary question I guess is: Why were you charged with the many Atomic Energy Act counts for which the penalty is life imprisonment, all of which the executive branch has now moved to dismiss and which I just dismissed?

During the proceedings in this case, I was told two things: first, the decision to prosecute you was made at the highest levels of the executive branch of the United States Government in Washington, D.C.

With respect to that, I quote from a transcript of the Aug. 15, 2000, hearing, where I asked this question. This was asked of Dr. Lee's lawyers: "Who do you contend made the decision to prosecute?"

Mr. Holscher responded: "We know that the decision was made at the highest levels in Washington. We know that there was a meeting at the White House the Saturday before the indictment, which was attended by the heads of a number of agencies. I believe the No. 2 and No. 3 persons in the Department of Justice were present. I don't know if the attorney general herself was present. It was actually held at the White House rather than the Department of Justice, which is, in our view, unusual circumstances for a meeting."

That statement by Mr. Holscher was not challenged.

The second thing that I was told was that the decision to prosecute you on the 39 Atomic Energy Act counts, each of which had life imprisonment as a penalty, was made personally by the president's attorney general.

In that respect, I will quote one of the assistant U.S. attorneys, a very fine attorney in this case -- this was also at the Aug. 15 hearing. This is talking about materials that I ordered to be produced in connection with Dr. Lee's motion relating to selective prosecution. The first category of materials involved the January 2000 report by the Department of Energy task force on racial profiling: "How would that in any way disclose prosecutorial strategy?"

Miss Fashing responded: "That I think falls more into the category of being burdensome on the government. I mean if the government -- if we step back for just a second -- I mean the prosecution decision and the investigation in this case, the investigation was conducted by the F.B.I., referred to the United States attorney's office, and then the United States attorney's office, in conjunction with -- well, actually, the attorney general, Janet Reno, made the ultimate decision on the Atomic Energy Act counts."

Dr. Lee, you're a citizen of the United States and so am I, but there is a difference between us. You had to study the Constitution of the United States to become a citizen. Most of us are citizens by reason of the simple serendipitous fact of our birth here. So what I am now about

to explain to you, you probably already know from having studied it, but I will explain it anyway.

Under the Constitution of the United States, there are three branches of government. There is the executive branch, of which the president of the United States is the head. Next to him is the vice president of the United States. The president operates the executive branch with his cabinet, which is composed of secretaries or heads of the different departments of the executive branch. The vice president participates in cabinet meetings.

In this prosecution, the more important members of the president's cabinet were the attorney general and the secretary of the Department of Energy, both of whom were appointed to their positions by the president.

The attorney general is the head of the United States Department of Justice, which despite its title, is a part of the executive branch, not a part of the judicial branch of our government.

The United States Marshal Service, which was charged with overseeing your pretrial detention, also is a part of the executive branch, not the judicial branch.

The executive branch has enormous power, the abuse of which can be devastating to our citizens.

The second branch of our national government is the legislative branch, our Congress. Congress promulgated the laws under which you were prosecuted, the criminal statutes. And it also promulgated the Bail Reform Act, under which in hindsight you should not have been held in custody.

The judicial branch of government, of which I am a member, is called the third branch of government because it's described in Article III of our Constitution.

Judges must interpret the laws and must preside over criminal prosecutions brought by the executive branch. Since I am not a member of the executive branch, I cannot speak on behalf of the president of the United States, the vice president of the United States, their attorney general, their secretary of the Department of Energy or their former United States attorney in this district, who vigorously insisted that you had to be kept in jail under extreme restrictions because your release pretrial would pose a grave threat to our nation's security.

I want everyone to know that I agree, based on the information that so far has been made available to me, that you, Dr. Lee, faced some risk of conviction by a jury if you were to have proceeded to trial. Because of that, I decided to accept the agreement you made with the United States executive branch under Rule 11(e)(1)(C) of the Federal Rules of Criminal Procedure.

Further, I feel that the 278 days of confinement for your offense is not unjust; however, I believe you were terribly wronged by being held in custody pretrial in the Santa Fe County Detention Center under demeaning, unnecessarily punitive conditions. I am truly sorry that I was led by our executive branch of government to order your detention last December.

Dr. Lee, I tell you with great sadness that I feel I was led astray last December by the executive branch of our government through its Department of Justice, by its Federal Bureau of Investigation and by its United States attorney for the district of New Mexico, who held the office at that time.

I am sad for you and your family because of the way in which you were kept in custody while you were presumed under the law to be innocent of the charges the executive branch brought against you.

I am sad that I was induced in December to order your detention, since by the terms of the plea agreement that frees you today without conditions, it becomes clear that the executive branch now concedes, or should concede, that it was not necessary to confine you last December or at any time before your trial.

I am sad because the resolution of this case drug on unnecessarily long. Before the executive branch obtained your indictment on the 59 charges last December, your attorney, Mr. Holscher, made a written offer to the office of the United States attorney to have you explain the missing tapes under polygraph examination.

I'll read from that letter of Dec. 10, 1999. I quote from that letter:

"Dear United States Attorney Kelly and First Assistant Gorence: I write to accept Mr. Kelly's request that we provide them with additional credible and verifiable information which will prove that Dr. Lee is innocent. On the afternoon of Wednesday, Dec. 8, Mr. Kelly informed me that it was very likely that Dr. Lee will be indicted within the next three to four business days. In our phone conversation, Mr. Kelly told me that the only way that we could prevent this indictment would be to provide a credible and verifiable explanation of what he described as missing tapes.

"We will immediately provide this credible and verifiable explanation. Specifically we are prepared to make Dr. Lee immediately available to a mutually agreeable polygraph examiner to verify our repeated written representations that at no time did he mishandle those tapes in question and to confirm that he did not provide the tapes to any third party.

"As a sign of our good faith, we will agree to submit Dr. Lee to the type of polygraph examination procedure that has recently been instituted at the Los Alamos Laboratory to question scientists. It is our understanding that the government has reaffirmed that this

new polygraph procedure is the best and most accurate way to verify that scientists are properly handling classified information."

At the inception of the December hearing, I asked the parties to pursue that offer made by Mr. Holscher on behalf of Dr. Lee, but that was to no avail.

MR. STAMBOULIDIS -- Your Honor, most respectfully, I take issue with that. There has been a full record of letters that were sent back and forth to you, and Mr. Holscher withdrew that offer.

JUDGE PARKER -- Nothing came of it, and I was saddened by the fact that nothing came of it. I did read the letters that were sent and exchanged. I think I commented one time that I think both sides prepared their letters primarily for use by the media and not by me. Notwithstanding that, I thought my request was not taken seriously into consideration.

Let me turn for the moment to something else. Although I have indicated that I am sorry that I was led by the executive branch to order your detention last December, I want to make a clarification here. In fairness, I must note that virtually all of the lawyers who work for the Department of Justice are honest, honorable, dedicated people, who exemplify the best of those who represent our federal government.

Your attorney, Mr. Holscher, formerly was an assistant United States attorney. The new United States attorney for the district of New Mexico, Mr. Norman Bay, and the many assistant United States attorneys here in New Mexico -- and I include in this Mr. Stamboulidis and Mr. Liebman, who are present here today -- have toiled long hours on this case in opposition to you. They are all outstanding members of the bar, and I have the highest regard for all of them.

It is only the top decision makers in the executive branch, especially the Department of Justice and the Department of Energy and locally, during December, who have caused embarrassment by the way this case began and was handled. They did not embarrass me alone. They have embarrassed our entire nation and each of us who is a citizen of it.

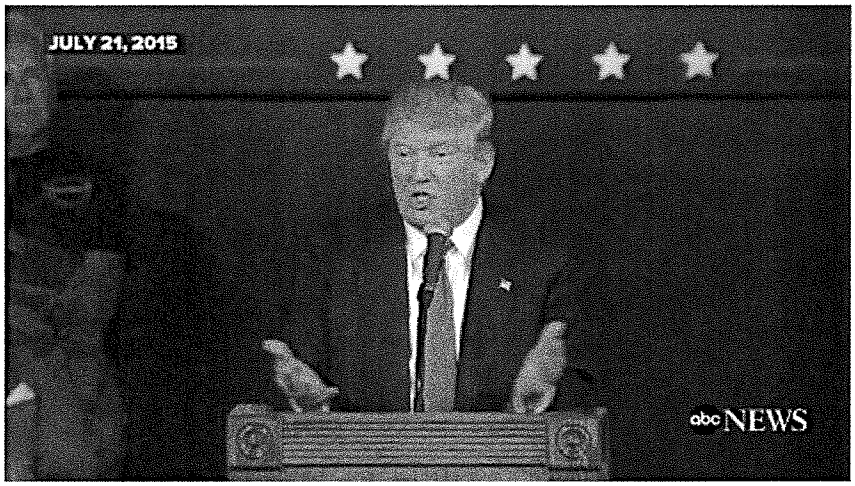
I might say that I am also sad and troubled because I do not know the real reasons why the executive branch has done all of this. We will not learn why because the plea agreement shields the executive branch from disclosing a lot of information that it was under order to produce that might have supplied the answer.

Although, as I indicated, I have no authority to speak on behalf of the executive branch, the president, the vice president, the attorney general, or the secretary of the Department of Energy, as a member of the third branch of the United States Government, the judiciary, the United States courts, I sincerely apologize to you, Dr. Lee, for the unfair manner you were held in custody by the executive branch.

10 times Trump attacked China and its trade relations with the US

Trump has a record of attacking China in unconventional ways.

By **VERONICA STRACQUALURSI**
November 9, 2017, 7:55 AM • 5 min read



President Trump's attacks on China

He has been after the superpower's economic policies since the start of his campaign.

— -- President Trump has long accused China of perpetrating one of the "greatest thefts in the history of the world" when it comes to trade with the U.S. and promised he would have his Treasury secretary label China a currency manipulator.

But while visiting China this week, Trump took a softer line and said the country was not responsible for trade imbalances with the U.S.

"I don't blame China," Trump said Thursday in Beijing. "After all, who can blame a country for being able to take advantage of another country to the benefit of its citizens?"

Instead, Trump pointed the finger at his predecessors for "allowing this out-of-control trade deficit to take place and to grow."

Trump's visit follows a presidential campaign in which he criticized China's business practices and how it handles trade with the United States. He has made China the target of more than 200 of his tweets over the years.

One the flip side, however, Trump said at a 2016 campaign rally that "I love China" and that he has made lots of money doing business with the country.

Top Stories

10 times Trump attacked China and its trade relations with the US
Nov 09, 7:55 AM

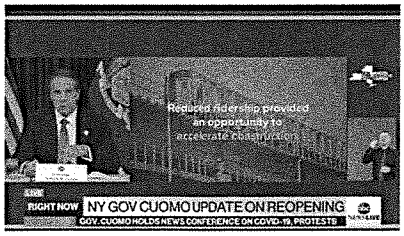
Coronavirus may have been in China in early fall, satellite data suggests
Jun 08, 6:04 AM

George Floyd protest updates: Trump reignites NFL feud in tweet aimed at commissioner
29 minutes ago

Trump's quest to 'dominate' amid protests sparks concerns about presidential powers
Jun 08, 4:14 AM

Cop charged after bodycam footage shows 'horrible use of force': Police chief
Jun 07, 4:45 PM

ABC News Live



24/7 coverage of breaking news and live events

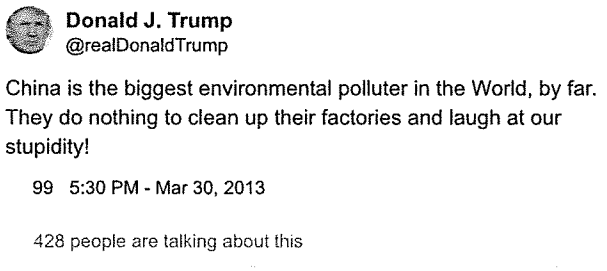
Here are some of the unconventional slights Trump has either said, written or tweeted about China in the past:

+ Trump: 'I don't blame China' for US-China trade imbalances

+ Trump's diplomatic dance on N. Korea tops agenda for meeting with Chinese president/> Campaign event in Bluffton, S.C. - July 21, 2015 "I beat the people from China. I win against China. You can win against China if you're smart. But our people don't have a clue. We give state dinners to the heads of China. I said why are you doing state dinners for them? They're ripping us left and right. Just take them to McDonald's and go back to the negotiating table." Campaign rally in Staten Island, N.Y. -- April 17, 2016 "China's upset because of the way Donald Trump is talking about trade with China. They're ripping us off, folks, it's time. I'm so happy they're upset." 'Crippled America' book - 2015 "There are people who wish I wouldn't refer to China as our enemy. But that's exactly what they are. They have destroyed entire industries by utilizing low-wage workers, cost us tens of thousands of jobs, spied on our businesses, stolen our technology, and have manipulated and devalued their currency, which makes importing our goods more expensive – and sometimes, impossible." <h3>'Good Morning America' interview - Nov. 3, 2015</h3> On labeling China an enemy "Because it's an economic enemy, because they have taken advantage of us like nobody in history. They have; it's the greatest theft in the history of the world what they've done to the United States. They've taken our jobs."

Twitter - March 30, 2013

"China is the biggest environmental polluter in the World, by far. They do nothing to clean up their factories and laugh at our stupidity!"



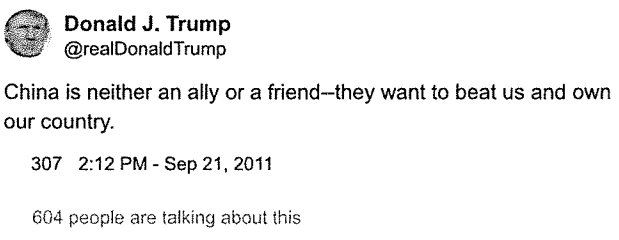
Campaign rally in Fort Wayne, Ind. - May 2, 2016

On China's trade policies

"We can't continue to allow China to rape our country and that's what they're doing. It's the greatest theft in the history of the world."

Twitter - Sept. 21, 2011

"China is neither an ally or a friend -- they want to beat us and own our country."

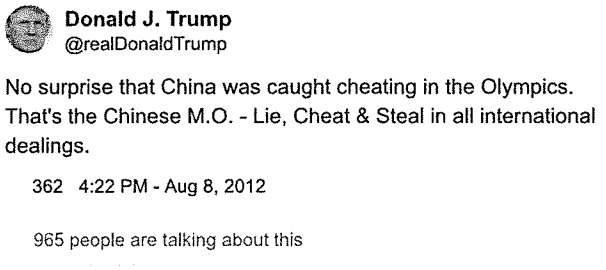


Campaign rally in Manchester, N.H. - June 20, 2016

"The single biggest weapon used against us and to destroy our companies is devaluation of currencies, and the greatest ever at that is China. Very smart, they are like grand chess masters. And we are like checkers players. But bad ones."

Twitter - Aug. 8, 2012

"No surprise that China was caught cheating in the Olympics. That's the Chinese M.O. - Lie, Cheat & Steal in all international dealings."



'Good Morning America' interview - Nov. 3, 2015

"But when you see China, these are fierce people in terms of negotiation. They want to take your throat out, they want to cut you apart. These are tough people. I've dealt with them all my life."

Comments (28)

abcNEWS

Before You Go

If You Like to Play, this Strategy Game is Addictive. No Install.
Forge of Empires - Free Online Game | Sponsored

New Portable AC Takes United States by Storm
WearableAC | Sponsored

These SUVs Are So Cool It's Hard to Believe They Cost Under $30K! Research Best Crossover SUV 2020
SUV | Sponsored

Massachusetts Launches New Policy For Cars Used Less Than 50 miles/day
Provide Insurance | Sponsored

If You Like to Play, this City-Building Game is a Must-Have. No Install.
Forge Of Empires | Sponsored

Startup Knocking Retirement Industry on Its Head
SmartAsset | Sponsored

Entire police department resigns at once, saying town 'seemingly cares so little about us'

NYC officer shot, killed while sitting in police vehicle

A Fast Way To Pay Off $10,000 in Debt
NerdWallet | Sponsored

New $89 Portable Air Cooler Is Taking United States By Storm
Blaux Portable AC | Sponsored

New $89 Portable AC Flying Off Shelves in United States
consumerbags.com | Sponsored

A Fast Way To Pay Off Up To $10,000 In Credit Card Debt
NerdWallet | Sponsored

New Senior Apartments in Boston Are Turning Heads
Senior Living | Search Ads | Sponsored

What Melissa Rivers Found Hidden in Joan Rivers' New York City Apartment

Kaepernick Faces Renewed Scrutiny as He Reclaims Job of Starting Quarterback

The Five Guys Ordering Secret You Need To Know
Wikibuy | Sponsored

The Cost of Renting a Private Jet Might Surprise You
Related Search Topics | Private Jet | Sponsored

Feeling A Little Anxious? Feals Can Help
FindKarma for Feals | Sponsored

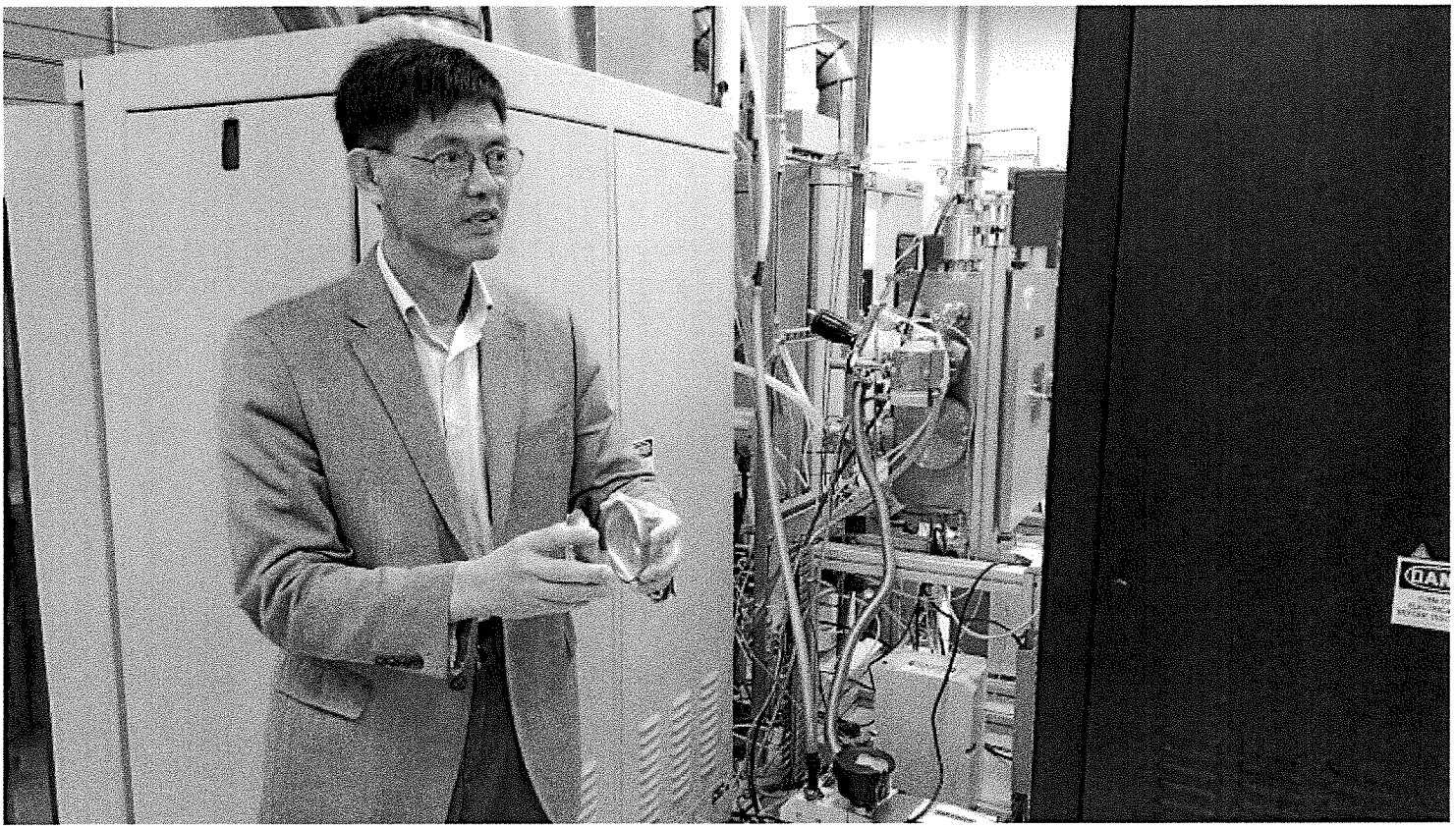
ABC News Network | Privacy Policy | Your CA Privacy Rights | Children's Online Privacy Policy | Interest-Based Ads | About Nielsen Measurement | Terms of Use | Do Not Sell My Info | Contact Us

Copyright © 2020 ABC News Internet Ventures. All rights reserved.

ADVERTISEMENT


CALIFORNIA

Is it police work or racial profiling? U.S. crackdown puts Chinese scholars on edge



Xiaoxing Xi, a Temple University physics professor, works with superconducting thin film in his lab. He is suing the federal government, which alleged in 2015 that he illegally sent technical information to China. The charges were dropped four months later. (Courtesy of Xiaoxing Xi)

By TERESA WATANABE
STAFF WRITER

JULY 22, 2019 | 5 AM

With three patents and more than 300 research papers to his name, Xiaoxing Xi was the respected chairman of Temple University's physics department.

That is until May 2015, when FBI agents burst into his home outside Philadelphia with guns drawn and accused him of being a spy. He was hauled away in handcuffs in front of his wife and young daughters, fingerprinted and strip-searched. He also was threatened with 80 years in prison and a $1-million fine.

Four months later, federal prosecutors dropped the charges after experts provided affidavits that the information Xi sent to scientists in China was widely known and publicly available on the internet. Federal authorities offered no apology, no explanation and no compensation — leaving Xi struggling to rebuild his shattered life.

Xi's case, and several others like it, have sparked widespread fears that the federal government's recent crackdown on China is leading to racial profiling of ethnic Chinese students and scholars. Xi was arrested during the Obama administration but pressure on China over trade, technology and security has intensified under President Trump, prompting federal officials to more aggressively police efforts to steal intellectual property and innovations.

ADVERTISING

Ads by Teads

One attorney, Peter Zeidenberg of Arent Fox in Washington, says he is defending about 20 ethnic Chinese scientists and scholars against charges related to China. His clients include Xi and Sherry Chen, who was a hydrologist with the National Weather Service when she was arrested in 2014. Five months later, federal prosecutors dropped all of the espionage-related charges against Chen but she is still fighting to get her job back. Both Xi and Chen are naturalized American citizens born in China.

"This is the broadest attack against Chinese Americans in recent memory," said Stewart Kwoh, executive director of Asian Americans Advancing Justice in Los Angeles, a legal defense and civil rights organization. "It's alarming to Chinese Americans to be swept up in this tension between the U.S. and China. Their civil rights are being abridged, but the tensions are so high people aren't finding a lot of support."

The Committee of Concerned Scientists, an international organization of leading scientists, physicians, engineers and scholars, sent a sharply worded letter to President Trump last month urging an immediate end to "the campaign of intimidation of ethnic Chinese scientists." The committee said they were being subjected to video surveillance and searches of their email accounts, correspondence and phone calls.

"Ethnic profiling and indiscriminate investigations of Chinese scientists have no place in our country," the letter said. "Besides damaging the image of the United States, it is also damaging to our national security by inflicting irreparable harm on some of our best scientists and making them think about leaving the country."

University leaders also are speaking out. MIT President L. Rafael Reif, in a letter to the campus community last month, warned that managing risks of academic espionage must not create a "toxic atmosphere of unfounded suspicion and fear" against ethnic Chinese researchers. He called "heartbreaking" reports from his faculty, researchers and students that they feel "unfairly scrutinized, stigmatized and on edge -- because of their Chinese ethnicity alone."

Federal officials, however, say the threat is real — and that they are colorblind in rooting it out.

Yi-Chi Shih, for example, was an adjunct UCLA professor of electrical engineering. He now faces up to 219 years in federal prison after being convicted last month of conspiring to export semiconductor chips with military applications to China. UCLA says his crimes were unrelated to his university work.

"We're looking for behavior, not individuals," said Michael Lauer, deputy director for extramural research at the National Institutes of Health, which has contacted 61 institutions about whether their scientists, most of them ethnic Chinese, followed all federal grant rules.

ADVERTISEMENT

NIH officials recently said in a letter to three ethnic Chinese scientific organizations that raised civil rights concerns that they would work to avoid "overreaction, stigmatization, harassment, and profiling" and "use our influence and bully pulpit as necessary to speak out against such prejudicial actions, for which there is no place in the biomedical research community." But the NIH letter, published in Science magazine in March, said that "instances have recently come to light where certain scientists, including some with links to foreign institutions and/or governments, have violated the honor-based systems and practices of the American research enterprise."

U.S. Rep. Judy Chu (D-Monterey Park) said she recently attended a federal intelligence briefing on Chinese threats to American universities and corporations, and agreed that concerns about Chinese efforts to steal U.S. intellectual property were legitimate. But she said the presentation failed to acknowledge the fears of racial profiling and gave the impression that "every Chinese person is evil and a spy."

Chu said she raised those concerns with intelligence officials. She said she does the same with her colleagues in Congress during her "never-ending effort" to bird-dog growing legislative efforts to require more scrutiny of Chinese students and scholars.

"I'm very concerned about an entire ethnic group [being] painted with a broad brush, where they're guilty until proven innocent," Chu said. "We're at a point where Chinese students and scholars could be guilty of the crime of studying while Chinese."

ADVERTISEMENT

The current political climate has unnerved even Leslie E. Wong, who retired this month as president of San Francisco State University. What used to be routine trips to China to attend university alumni events have become fraught with anxiety, he said.

"The paranoia started seeping in," Wong said. "You think, 'Oh my god. The records show I go to China.' You become sensitive to the fact that your last name is Wong and you go to Asia. It's sort of a niggling thing in your head that says let's be careful, keep extra diary notes, keep all of our I's dotted and Ts crossed."

This isn't the first time that the ethnic Chinese community has been unfairly targeted during times of tension with China, said Charlie Woo, public policy chairman of the Committee of 100, a national organization of leading Chinese Americans.

One of the earliest cases involved Qian Xuesen, a prominent Chinese scientist at MIT and Caltech who was accused of being a communist sympathizer and stripped of his security clearance in 1950, despite protests by his colleagues. After five years under house arrest, he returned to China in 1955 and helped lead development of the Chinese nuclear weapons program, becoming known as the "Father of Chinese Rocketry."

ADVERTISEMENT

In 1999, a Taiwanese American scientist, Wen Ho Lee, was indicted by a federal grand jury on charges of stealing U.S. nuclear secrets for China while working at the Los Alamos National Laboratory in New Mexico. The following year, federal prosecutors dropped all but one of the 59 charges, with Lee pleading guilty to one charge of mishandling sensitive documents after spending months in solitary confinement.

Woo said the federal crackdown is driving away top scientists, such as Chunzai Wang, one of the world's leading experts on climate change who worked for 17 years for the National Oceanic and Atmospheric Administration. Wang, a naturalized U.S. citizen, was

accused of taking a salary from a source other than the U.S. government while serving as a guest professor at a Chinese university. In a plea deal last year, Wang pleaded guilty to one felony charge and returned to China, where he is continuing his research.

To address the rising unease among ethnic Chinese, Woo is planning a major symposium on racial profiling this fall in Silicon Valley.

As for Xi, the scientist said the false arrest has forever altered his life. He lost his university chairmanship and most of his nine federal research grants and contracts. He says he can't sleep soundly or concentrate, losing the laser-focused mind that helped him excel in science.

ADVERTISEMENT

Xi is suing the federal government but faces $220,000 in legal bills.

"Everything that I worked on for 30 years could be gone — my career, reputation, livelihood," Xi said. "But if I can help the Chinese American community and the scientific community to become more aware of what's going on and speak up, then there will be something positive to come out of this."

Times staff writer Don Lee contributed to this report.

CALIFORNIA | EDUCATION

The stories shaping California

Get up to speed with our Essential California newsletter, sent six days a week.

Enter Email Address

SIGN ME UP

You may occasionally receive promotional content from the Los Angeles Times.

Teresa Watanabe

Twitter Instagram Email Facebook

Teresa Watanabe covers education for the Los Angeles Times. Since joining the Times in 1989, she has covered immigration, ethnic communities, religion, Pacific Rim business and served as Tokyo correspondent and bureau chief. She also covered Asia, national affairs and state government for the San Jose Mercury News and wrote editorials for the Los Angeles Herald Examiner. A Seattle native, she graduated from USC in journalism and in East Asian languages and culture.

SUBSCRIBERS ARE READING

OPINION

Op-Ed: Kareem Abdul-Jabbar: Don't understand the protests? What you're seeing is people pushed to the edge

FOOD

Here's a list of more than 200 black-owned food businesses in L.A.

OPINION

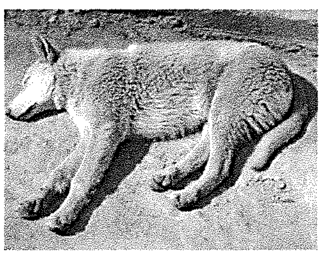
Joe Biden: To end systemic racism, no o can stay silent. No one can ignore injustice

TRAVEL

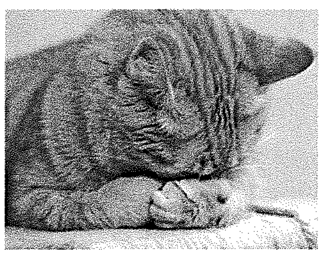
What's open and closed this weekend: Parks, trails and beaches in Southern California

Around the Web

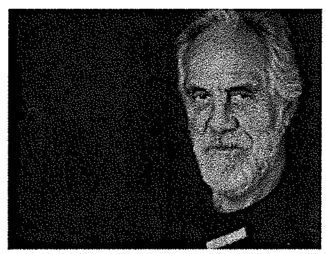
Ads by Revcontent



How Dogs Cry For Help: 3 Warning Signs Your Dogs Is Crying For Help
DR. MARTY



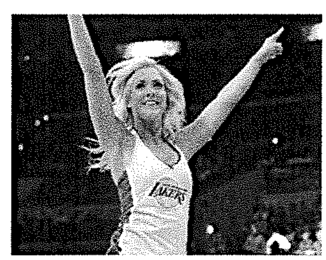
3 Ways Your Cat Asks for Help
DR. MARTY



"They Almost Killed Me" Why Tommy Chong Doesn't Trust CBD
TOMMY CHONG

Costco Workers Reveal 14 Things They'd Never Buy
BETTERBE

20 Places Where $150K Is More Than Enough To Retire
MONEYWISE.COM



Fastest Shrinking Cities In America: City In Massachusetts Tops The List
UNPUZZLE FINANCE

CORONAVIRUS >

L.A. County coronavirus cases near 64,000 amid protests and reopenings

She's patrolled the Navajo Nation for nearly 20 years. Nothing prepared her for the COVID-19 outbreak

California could reopen gyms, bars and professional sports soon but warns 'guidance doesn't mean go'

L.A. is less cautious than Bay Area in coronavirus reopening. Here's why the two regions diverged

Tracking California's path to reopening, plus news, advice and distractions (free)

Cases statewide »

130,930	4,633
confirmed	deaths

As of June 7, 10:38 p.m. Pacific

ADVERTISEMENT

LATEST CALIFORNIA >

CALIFORNIA

Massive Hollywood protest shows the staying power of the George Floyd movement

17 minutes ago

CALIFORNIA

Wind-driven fire breaks out in Castaic, burns near 5 Freeway

1 hour ago

CALIFORNIA

Store manager, bloodied in assault by customer, describes life in the age of COVID-19

1 hour ago

CALIFORNIA

Coronavirus transmission rate climbing in L.A. County as economy reopens

1 hour ago

BOOKS

Excerpt: Cowboys in Compton find hope and healing on horseback

1 hour ago

ADVERTISEMENT

Get our free Coronavirus Today newsletter

Sign up for the latest news, best stories and what they mean for you, plus answers to your questions.

Enter Email Address

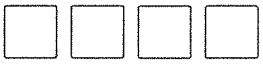
SIGN ME UP

You may occasionally receive promotional content from the Los Angeles Times.

ADVERTISEMENT

Subscribe for unlimited access

Follow Us



Copyright © 2020, Los Angeles Times | Terms of Service | Privacy Policy | CA Notice of Collection | Do Not Sell My Info

Center for Strategic and International Studies

TRANSCRIPT

China Initiative Conference

"Opening Remarks"

EVENT DATE
Thursday, February 6, 2020

TIME
8:30 a.m. EDT

LOCATION
2nd Floor, CSIS Headquarters, Washington, D.C.

FEATURING
Speaker
Christopher Wray
Director of the Federal Bureau of Investigation (FBI)

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

Christopher Wray: Well, thanks, John. And I want to add my thanks to those of others to CSIS for hosting this event and for all you to do educate policymakers and the public.

You've just heard a pretty sobering presentation from Bill about some of the costs and the impact of this threat. I will tell you from my lens, having been FBI Director for over two years now and having had to confront what I would argue is a wider than ever array of challenging threats, this one to me really stands out as the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality.

And this is a threat, as I think you heard from Bill, not just to our economic security, but by extension to our national security. And I believe that to respond to the China threat more effectively we need to better understand several key aspects of it. So, what I thought I'd try to do is help further set the table for today's presentations and give you a little bit of a window into how the FBI sees the threat and how we're dealing with it.

The first thing I think we need to understand about the threat from China is just how diverse and multilayered it is. And I say that in terms of its techniques, its actors, and in its targets. China is using a wide range of methods and techniques. And I'm talking about everything from cyber intrusions to corrupting trusted insiders. They've even engaged in outright physical theft. And they've pioneered an expansive approach to stealing innovation through a wide range of actors, including not just Chinese intelligence services but state-owned enterprises, ostensibly private companies, certain kinds of graduate students and researchers, and a whole variety of other actors all working on their behalf.

But it's also a diverse threat when it comes to the sectors and sizes of China's targets here in the U.S. We're talking about everything from Fortune 100 companies to Silicon Valley startups, from government and academia to high tech, and even agriculture. Even as I stand here talking with you today, the FBI has about a thousand investigations involving China's attempted theft of U.S.-based technology in all 56 of our field offices and spanning just about every industry and sector.

They're not just targeting defense-sector companies. The Chinese have targeted companies producing everything from proprietary rice and corn seeds to software for wind turbines to high-end medical devices. And they're not just targeting innovation and R&D. They're going after cost and pricing data, internal strategy documents, bulk PII; really just about anything that can give them a competitive advantage.

They're also targeting cutting-edge research at our universities. Just last week, for example, we announced charges against the chairman of Harvard's chemistry department for false statements related to a Chinese talent plan and a PLA officer at Boston University for concealing her military ties. In December, we arrested a Chinese researcher for smuggling vials of stolen biological research.

Now, all three of those cases were just investigated by one of our field offices, one of our 56 field offices, the Boston field office, in about a month. So, it gives you a taste of what we're dealing with. And you'll hear more about some of these cases

later this morning. But in sum, the Chinese government is taking an all-tools and all-sectors approach, and that depends on our end our own all-tools and all-sectors approach in response.

The second thing I think we really need to understand about this threat is the scope of China's ambitions, which are no secret. You heard a little bit about that from Bill already. To be clear, this is not about the Chinese people as a whole, and it sure as heck is not about Chinese Americans as a group. But it is about the Chinese government and the Chinese Communist Party.

The Chinese government is fighting a generational fight to surpass our country in economic and technological leadership, but not through legitimate innovation, not through fair, lawful competition, and not by giving their citizens the freedom of thought and speech and creativity that we treasure here in the United States. Instead they've shown that they're willing to steal their way up the economic ladder at our expense.

In recent decades, China has grown its economy rapidly by combining low-cost Chinese labor with Western capital and technology. But China's leaders know they can't rely on that model forever. To surpass America, they need to make leaps in cutting-edge technologies.

Last March, at a Communist Party gathering, Chinese Premier Li made that understanding pretty clear. He said, and I quote, our capacity for innovation is not strong and our weakness in terms of core technologies for key fields remains a salient problem.

To accomplish the breakthroughs they seek, China is acquiring intellectual property from America and innovation by any means necessary. We see Chinese companies stealing American intellectual property to avoid the hard slog of innovation and then using it to compete against the very American companies they victimize; in effect, cheating twice over.

Part of what makes this threat so challenging is that the Chinese are using an expanding set of nontraditional methods, both lawful and unlawful – so blending things, on the one hand, like foreign investments and corporate acquisitions with, on the other hand, things like cyber intrusions and espionage by corporate insiders. Their intelligence services also increasingly hire hacking contractors who do the government's bidding to try to obfuscate the connection between the Chinese government and the theft of our data.

The Chinese government is clearly taking the long view here, and in many ways, that's an understatement. I would argue they've made the long view an art form. They are calculating, they are persistent, they are patient.

The third thing we need to remember about this threat is that China has a fundamentally different system than ours, and they are doing all they can to exploit the openness of ours. Many of the distinctions that we hold dear and that are so ingrained in the way we operate in this country are blurred – if they exist at all – in China. I'm talking about distinctions between the Chinese government and the Chinese Communist Party, distinctions between civilian and military sectors or uses, distinctions between the state and their business sector. For one thing, many

large Chinese businesses are state-owned enterprises – literally owned by the government and thus the party. And even where not formally owned, they are legally and practically beholden to the government in a very tangible way, and you've heard a little bit about that from Bill just a few minutes ago.

And you don't have to take my word for it; you can take theirs. China, as you heard, has national security laws that compel Chinese companies to provide their government with information and access at their government's request. And virtually all Chinese companies of any size are required to have Communist Party cells inside them to make sure that those companies stay in line with the party's principles and policies. Try to wrap your brain around something like that happening in our system. You can't.

Unfortunately, it's a similar story in the academic sphere. The Chinese government doesn't play by the same rules of academic integrity and freedom that the U.S. does. We know they use some Chinese students in the U.S. as nontraditional collectors of our intellectual property. We know that through their Thousand Talents Plans and similar programs, they try to entice scientists at our universities to bring their knowledge back to China, even if that means – even if that means stealing proprietary information or violating export controls or conflict-of-interest policies to do so. And we know they support the establishment of institutes on our campuses that are more concerned with promoting Communist Party ideology than independent scholarship. We also know that they pressure Chinese students to self-censor their views while studying here and that they use campus proxies to monitor both U.S. and foreign students and staff. And last, we know that they use financial donations as leverage to discourage American universities from hosting speakers with views the Chinese government doesn't like.

So, whether we're talking about the business world or the academic world, it is crucial that we acknowledge and understand these differences between our two systems because China is doing everything, they can to turn those differences to their advantage. Obviously, they're exploiting our open academic environment for research and development. They are exploiting American companies' openness for foreign investment and partnership, and they are acquiring U.S. firms to gain ownership of what those firms have created.

Meanwhile, they take advantage of their own system being closed. They often require our businesses to put their trade secrets and their customers' personal data at risk as the cost of gaining access to China's huge market. And they make American joint ventures operating in China establish those Communist Party cells within their companies.

This government control over our joint ventures has become so common that a lot of American companies don't even really stop to think about it. But if these companies want to protect their information, they sure better be thinking about it. They should also be thinking about what it means to operate in an environment where a major IT provider like Huawei with broad access into so much that U.S. companies do in China has been charged with fraud, obstruction of justice, and theft of trade secrets. There's no reason for any U.S. company working in China to think that it's safely off-limits. So, understanding the Chinese counterintelligence threat better will help us respond to it more effectively.

As I described, China is taking a multifaceted response, so we've got to have a multifaceted response on our end. Our folks at the FBI and DOJ are working their tails off every day to protect our nation's companies, our universities, our computer networks, and our ideas and innovation. To do that we're using a broad set of techniques, from our traditional law enforcement authorities to our intelligence capabilities. And you'll hear more about that in the panels later this morning, but I'll briefly note that we're having real success and real impact.

With the help of so many of our foreign partners, we've arrested targets all over the globe. Our investigations and prosecutions have exposed the tradecraft and techniques the Chinese are using, raising awareness of the threat and our industries' defenses. They also show our resolve and our ability to attribute these crimes to those responsible. We've seen how our criminal indictments have rallied other nations to our cause, which is crucial to persuading the Chinese government to change its behavior.

We're also working more closely than ever with partner agencies here in the U.S. and with our partners abroad. We've got a whole host of tools we can use, from criminal charges and civil injunctions to things like economic sanctions, entity listings, visa revocations. We're also working with CFIUS – the Committee on Foreign Investment in the United States – in its review of foreign investments in American companies that produce critical technologies or collect sensitive personal data of U.S. citizens.

But we can't do it on our own. We need a whole-of-society response with government and the private sector and the academic sector all working together. That's why we in the intelligence and law enforcement communities are working harder than ever to give companies and universities the information they need to make informed decisions on their own to protect their most valuable assets.

Through our Office of Private Sector, the FBI has stepped up our national outreach to spread awareness of this threat. For example, we're holding conferences for members of our DSAC – our Domestic Security Alliance Council – where we share information with Fortune 1000 companies about China's continued efforts to steal intellectual property. We also now have private-sector coordinators in each of the FBI's 56 field offices who lead our engagement with local businesses and universities. We're meeting with these partners frequently, providing threat awareness briefings, and helping connect them to the right people in the FBI on any concern.

Our Office of the Private Sector also engages with a variety of academic associations on the China threat, including the American Council on Education, the Association of American Universities, and the Association of Public and Land Grand Universities. Just last October at FBI Headquarters we hosted an academia summit where more than 100 attendees discussed how the academic community can continue to work with the FBI and other federal agencies to tackle national security threats on our campuses.

All of this outreach is geared towards helping our partners take the long view and preventing our openness from being exploited. In this country we value our open free-market system, including the way it attracts international investment and talent to our country. In this country we value academic freedom, including

international collaboration and the benefits we gain from having talented students from abroad – including China – come here to study. We're not going to change the way we are or who we are, but at the same time we've got to be clear-eyed and thoughtful about the threat from China and do everything possible to ensure a level playing field between our two countries.

So the FBI is encouraging our business and academic partners to keep that long view in mind when engaging with China. We're asking executives and boards of directors to carefully consider who they choose to do business with and who they make part of their supply chains. A decision to enter into a joint venture or contract with a particular vendor might look good to them in the near term, might make a lot of money today, might sound great on the next earnings call, but it might not look so hot a few years down the road when they find themselves bleeding intellectual property or hemorrhaging some of their most sensitive data.

We're also encouraging universities to take steps to protect their students from intimidation or control by foreign governments and to give them ways to report such incidents. We're urging universities to seek transparency and reciprocity in their agreements with foreign institutions, and to do their due diligence on the foreign nationals they allow to work and study on their campuses.

Finally, we're asking our private sector and academic partners to reach out to us if they see something that concerns them. And we're going to keep working to build trusted relationships with them so that they know with confidence that we're here to help.

Let me close by making one thing clear: confronting this threat effectively does not mean we shouldn't do business with the Chinese, does not mean we shouldn't host Chinese visitors, does not mean we shouldn't welcome Chinese students or coexist with China on the world stage. But what it does mean is that when China violates our criminal laws and well-established international norms, we are not going to tolerate it, much less enable it. The Department of Justice and the FBI are going to hold people accountable for that and protect our nation's innovation and ideas.

Thanks for having me here today. (Applause.)

(END)

World

US trade adviser links virus to China government

JUNE 22, 2020

WASHINGTON — White House trade adviser Peter Navarro is calling the coronavirus a "product of the Chinese Communist Party" and suggesting without evidence it may have been intentionally created by the Chinese government.

Navarro said on CNN's "State of the Union" that it remains unclear how the virus started and "until we get some information about what happened in those labs or what happened in that wet market, we know that the virus was spawned in China."

President Trump and his allies have been repeating the unsubstantiated theory linking the outbreak's origin to a possible accident at a Chinese virology laboratory. US officials describe the evidence as purely circumstantial.

The leading theory is that infection among humans began at an animal market in Wuhan.

ADVERTISING

Navarro says it's an "open question" whether the virus was purposefully created. He said that, in his view, the Chinese government is "guilty until proven innocent."

Associated Press

Watchdogs say Treasury too secretive on business loans

NEW YORK — The Trump administration has relented to public pressure and pledged to provide more details about which small businesses received loans from a $600 billion-plus coronavirus aid program. But government watchdogs say even more transparency is needed to get an accurate picture of who was helped, and who was left out.

Under pressure from Democratic lawmakers and government watchdogs, the Treasury Department and the Small Business Administration said Friday that they would disclose the names of small-business owners who received $150,000 or more in forgivable loans.

But for loans of less than $150,000, the agencies will not name the recipients, revealing only summary information broken down by ZIP code, industry, and demographics.

Specialists say this could paint an incomplete or misleading picture. Recipients of smaller loans could be part of a bigger subsidiary that would be hidden, and it won't be clear what percentage of loans went to minority-owned businesses. A factory in a minority neighborhood, for example, could be owned by an individual or conglomerate based elsewhere.

The Treasury Department didn't respond to a request for comment. Secretary Steven Mnuchin has previously said he is concerned about business owners' privacy.

Associated Press

Hundreds test positive at Tyson Foods plant in Ark.

ST. PETERSBURG, Fla. — Tyson Foods is looking into reports that China's customs agency has suspended poultry imports from a Tyson facility in the United States after coronavirus cases were confirmed among its employees.

A Tyson spokesman said Sunday that the plant in question is in Springdale, Ark.

The announcement out of China gave no details of the quantity of meat affected.

On Friday, Tyson Foods announced the results of coronavirus testing at its facilities in Benton and Washington counties, Arkansas, and said that about 95 percent of employees who ultimately tested positive for the virus didn't show any symptoms. Of the 3,748 employees tested, 481 tested positive for COVID-19, and 455 were asymptomatic.

There have been several other COVID-19 outbreaks at Tyson plants around the United States, including in North Carolina, Nebraska, and Iowa.

Associated Press

© 2020 Boston Globe Media Partners, LLC